



ENVCWI-PTG1

Wireless Network (IP) Camera with
PAN & TILT

Advanced Installation Guide

Version 1.1

Regulatory notes and statements

Wireless LAN, Health and Authorization for use

Radio frequency electromagnetic energy is emitted from Wireless LAN devices. The energy levels of these emissions however are far much less than the electromagnetic energy emissions from wireless devices like for example mobile phones. Wireless LAN devices are safe for use frequency safety standards and recommendations. The use of Wireless LAN devices may be restricted in some situations or environments for example:

- On board of airplanes, or
- In an explosive environment, or
- In case the interference risk to other devices or services is perceived or identified as harmful

In case the policy regarding the use of Wireless LAN devices in specific organizations or environments (e.g. airports, hospitals, chemical/oil/gas industrial plants, private buildings etc.) is not clear, please ask for authorization to use these devices prior to operating the equipment.

Regulatory Information/disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The Manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, of the substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

USA-FCC (Federal Communications Commission) statement

This device complies with Part 15 of FCC Rules.

Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of this device.

FCC Radio Frequency Exposure statement

This Wireless LAN radio device has been evaluated under FCC Bulletin OET 65 and found compliant to the requirements as set forth in CFR 47 Sections 2.1091, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices. The radiated output power of this Wireless LAN device is far below the FCC radio frequency exposure limits. Nevertheless, this device shall be used in such a manner that the potential for human contact during normal operation is minimized.

When nearby persons has to be kept to ensure RF exposure compliance, in order to comply with RF exposure limits established in the ANSI C95.1 standards, the distance between the antennas and the user should not be less than 20 cm.

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the instructions, it may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the distance between the equipment and the receiver.
3. Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

Export restrictions

This product or software contains encryption code that may not be exported or transferred from the US of Canada without an approved US Department of Commerce export license.

Safety Information

Your device contains a low power transmitter. When device is transmitted it sends out radio frequency (RF) signal.

CAUTION: To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use on the supplied antenna.

Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.

The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Protection requirements for health and safety – Article 3.1a

Testing for electric safety according to EN 60950 has been conducted.

These are considered relevant and sufficient.

Protection requirements for electromagnetic compatibility (EMC) – Article 3.1b

Testing for electromagnetic compatibility according to EN 301 489-1, EN 301 489-17 and EN 55024 has been conducted. These are considered relevant and sufficient.

Effective use of the radio spectrum – Article 3.2

Testing for radio test suites according to EN 300 328 has been conducted.

These are considered relevant and sufficient.

CE in which Countries where the product may be used freely:

Germany, UK, Italy, Spain, Belgium, Netherlands, Portugal, Greece, Ireland, Denmark, Luxembourg, Austria, Finland, Sweden, Norway and Iceland.

France: except the channel 10 through 13, law prohibits the use of other channels.

Caution

The Federal Communication Commission warns the user that changes or modifications to the device not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Copyright

The company has an on-going policy of upgrading its products and it may be possible that information in this document is not up-to-date. Please check with your local distributors for the latest information.

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission or consent from the company.

Trademarks

All products, companies and brand names are trademarks or registered trademarks of their respective companies. They are used for identification purpose only.

Specifications are subject to be changed without prior notice.

PREFACE

Thank you for purchasing the Wireless Network (IP) Camera with PAN & TILT, a powerful wireless network camera with the 2-way audio function which provides the high-quality image and on-the-spot audio via the Internet connection. The camera's pan/tilt functions allow you to control the camera to monitor everywhere remotely. Through the GPIO connectors, the camera can attach a variety of external devices for your specific purposes. The camera can be installed as a standalone system within your application environment easily and quickly, and supports remote management function so that you can access and control it using a Web browser on your PC. This *Advanced Installation Guide* provides you with the instructions and illustrations on how to use your camera, which includes:

- Chapter 1 Introduction to Your Camera** describes the features of the camera. You will also know the components and functions of the camera.
- Chapter 2 Hardware Installation** helps you install the camera according to your application environment. You can use this camera at home, at work, at any where you want.
- Chapter 3 Accessing the Camera** lets you start using your camera without problem. The camera can be set up easily and work within your network environment instantly.
- Chapter 4 Configuring the Camera** guides you through the configuration of the camera using the Web browser on your PC.
- Chapter 5 Appendix** provides the specification of the camera and some useful information for using your camera.

NOTE The illustrations and configuration values in this guide are for reference only. The actual settings depend on your practical application of the camera.

Contents

- Preface.....5
- Chapter 1 Introduction To Your Camera.....7
 - 1.1 Checking the Package Contents.....7
 - 1.2 Getting to Know Your Camera8
 - 1.3 Features and Benefits10
 - 1.4 System Requirement.....12
- Chapter 2 Hardware Installation13
 - 2.1 Installing the Wall Mount Kit.....13
 - 2.2 Connecting the Camera to LAN/WLAN.....14
 - 2.3 Applications of the Camera15
- Chapter 3 Accessing The Camera.....16
 - 3.1 Using IPFinder16
 - 3.2 Accessing to the Camera17
 - 3.3 Configuring the IP Address of the PC21
- Chapter 4 Configuring The Camera.....22
 - 4.1 Using the Web Configuration22
 - 4.2 Using Smart Wizard23
 - 4.3 Basic Setup26
 - 4.4 Network Settings30
 - 4.5 Pan/Tilt Settings37
 - 4.6 Setting up Video & Audio38
 - 4.7 Event Server Configuration42
 - 4.8 Motion Detect.....45
 - 4.9 Event Config.....46
 - 4.10 Tools51
 - 4.11 Information53
- Appendix.....54
 - A.1 Specification.....54
 - A.2 GPIO Terminal Application.....56
 - A.3 Glossary of Terms.....57

CHAPTER 1

INTRODUCTION TO YOUR CAMERA

1.1 Checking the Package Contents

Check the items contained in the package carefully. You should have the following:

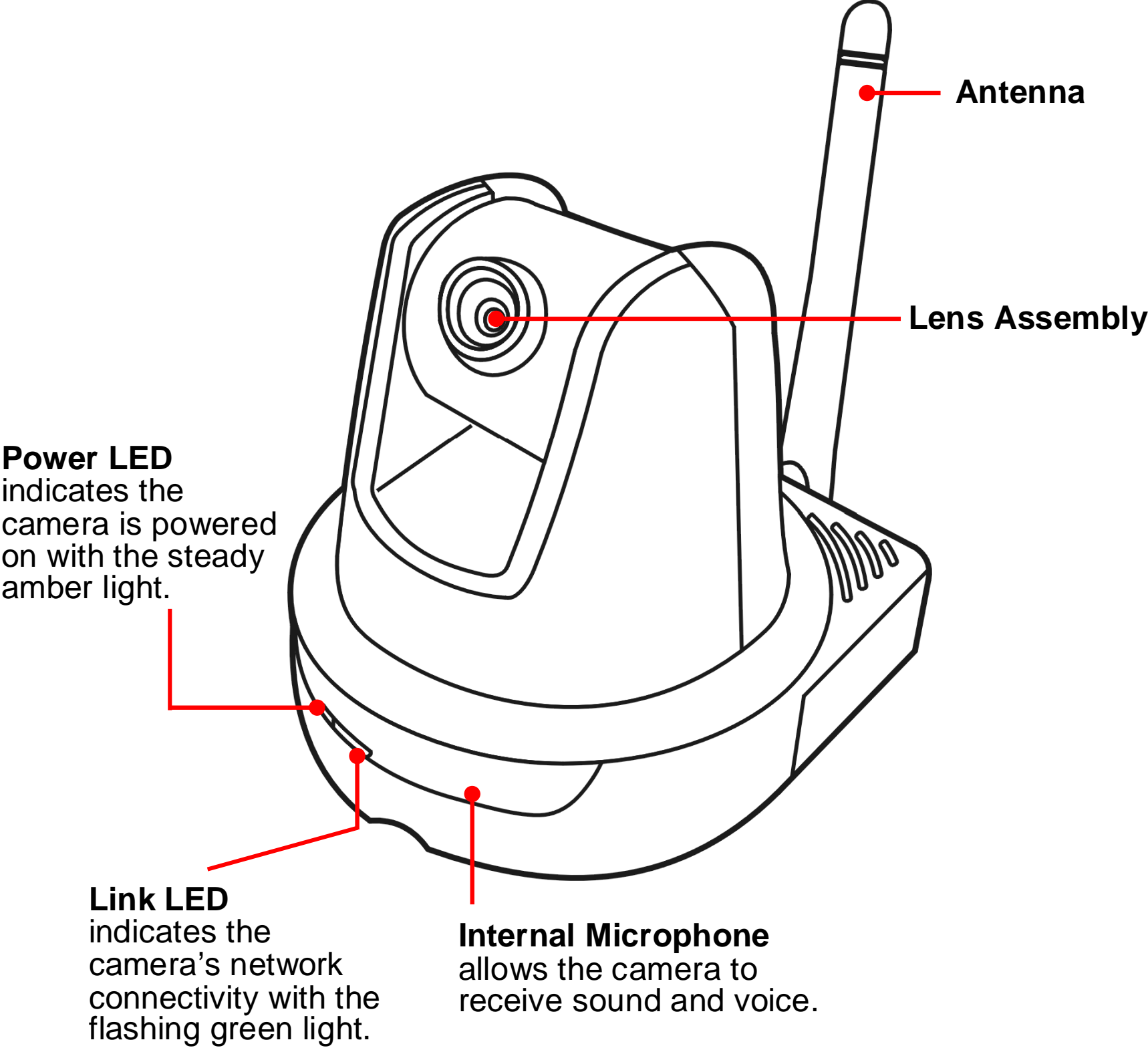
- ☒ One Wireless Network (IP) Camera with PAN & TILT.
- ☒ One AC Power Adapter.
- ☒ One External Detachable Antenna
- ☒ One Wall Mount Kit.
- ☒ One GPIO Connector
- ☒ One Ethernet Cable (RJ-45 type).
- ☒ One Installation CD-ROM.
- ☒ One *Quick Installation Guide*.

NOTE Once any item contained is damaged or missing, contact the authorized dealer of your locale.

If you have any problem on the product(s), please contact your local authorized dealer or check our web site

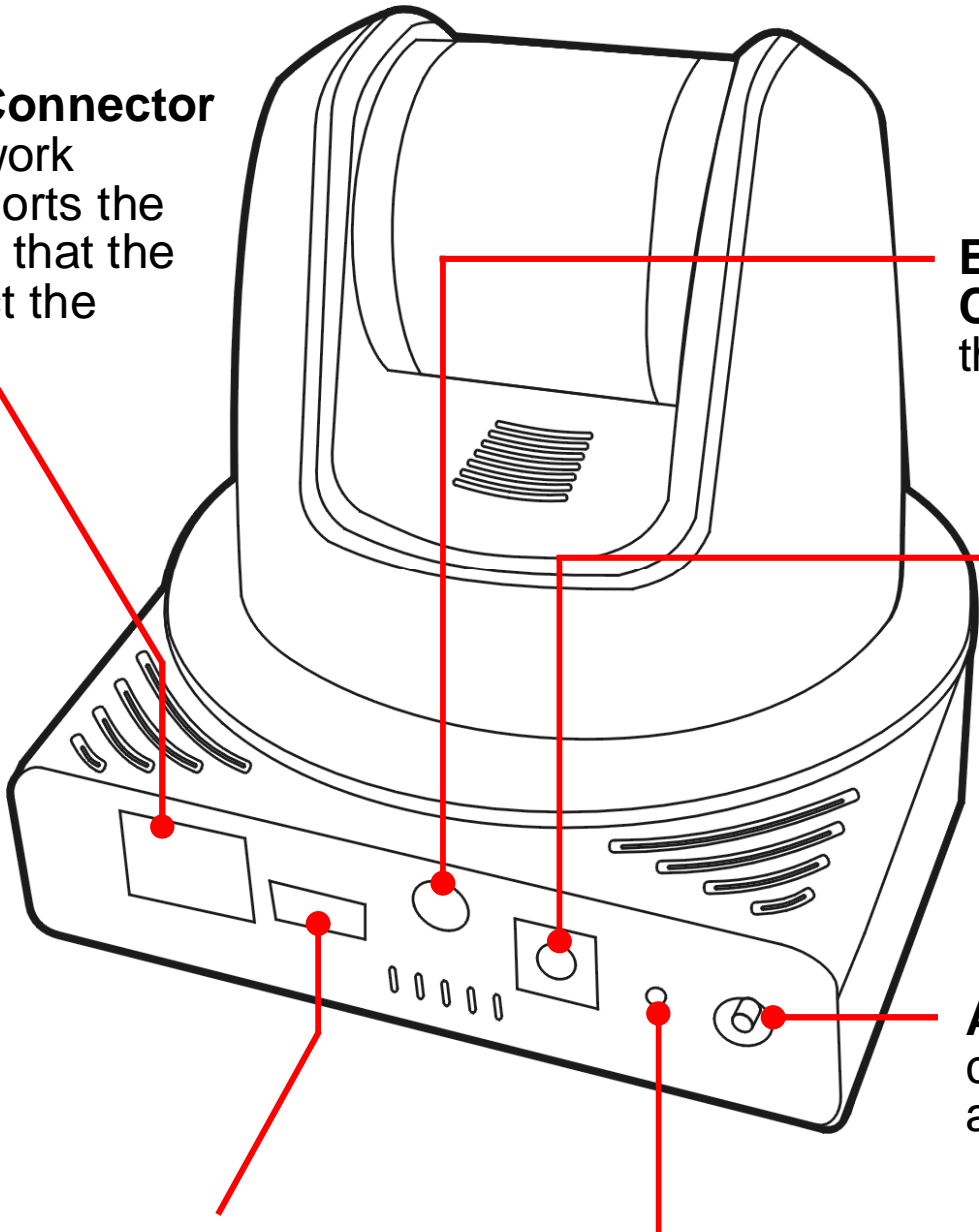
<http://www.encore-usa.com> for support.

1.2 Getting to Know Your Camera



Front View

Ethernet Cable Connector
connects the network
cable, which supports the
NWay protocol so that the
camera can detect the
network speed
automatically.



**External Antenna
Connector** connects
the external antenna.

DC Power Connector
connects the AC
power adapter, in
order to supply power
to the camera.

Audio-out Connector
connects an external
active speaker.

GPIO Connectors
is used to connect the
external devices.

Reset Button
will restart the camera when it
is pressed quickly; when it is
pressed and held for five
seconds, the camera will
resume the factory default
settings.

Rear View

1.3 Features and Benefits

■ **MJPEG codec Supported**

The camera provides you with excellent images by the MJPEG codec technology, allowing you to adjust image size and quality, and bit rate according to the networking environment.

■ **2-way Audio Capability**

The built-in microphone of the camera provides on-the-spot audio via the Internet, allowing you to monitor the on-site voice. In addition, you can connect an external speaker to the camera to speak through the camera.

■ **Optimal Viewing**

With the pan/tilt functions, you can easily monitor everywhere via the camera by moving the camera lens to the left/right (165/165 degrees) or up/down (90/15 degrees). In addition, you can assign up to eight positions for the camera, enabling you to move the camera lens to the desired position quickly.

■ **I/O Connectors Provided**

The camera provides the I/O connectors on the rear panel (IN/OUT), which provide the physical interface to send and receive digital signals to a variety of external alarm devices. You can connect a special featured device, and then configure the settings and control the device from the **GPIO Trigger** window of Web Configuration.

■ **Remote Control Supported**

By using a standard Web browser or the bundled UltraView software application, the administrator can easily change the configuration of the camera via Intranet or Internet. In addition, the camera can be upgraded remotely when a new firmware is available. The users are also allowed to monitor the image and take snapshots via the network.

■ **Multiple Platforms Supported**

The camera supports multiple network protocols, including TCP/IP, SMTP e-mail, HTTP, and other Internet related protocols. Therefore, you can use the camera in a mixed operating system environment, such as Windows 2000 and Windows XP.

■ **Multiple Applications Supported**

Through the remote access technology, you can use the cameras to monitor various objects and places for your own purposes.

For example, babies at home, patients in the hospital, offices and banks, and more. The camera can capture both still images and video clips, so that you can keep the archives and restore them at any time.

1.4 System Requirement

■ Networking

LAN: 10Base-T Ethernet or 100Base-TX Fast Ethernet.
WLAN: IEEE 802.11g/b compliant wireless interface.

■ Accessing the Camera using Web Browser

Platform: Microsoft® Windows® 2000/XP/Vista
CPU: Intel Pentium III 350MHz or above
RAM: 128MB
Resolution: 800x600 or above
User Interface: Microsoft® Internet Explorer 6.0 or above
Apple Safari 2 or above
Mozilla Firefox 2.00 or above

■ Accessing the Camera using UltraView

Platform: Microsoft® Windows® 2000/XP/Vista
Hardware Requirement:
1 camera connected: Intel Pentium III 800MHz; 512MB RAM
2 ~ 4 cameras connected: Intel Pentium 4 1.3GHz; 512MB RAM
5 ~ 8 cameras connected: Intel Pentium 4 2.4GHz; 1GB RAM
9 ~ 16 cameras connected: Intel Pentium 4 3.4GHz; 2GB RAM
Resolution: 1024x768 or above

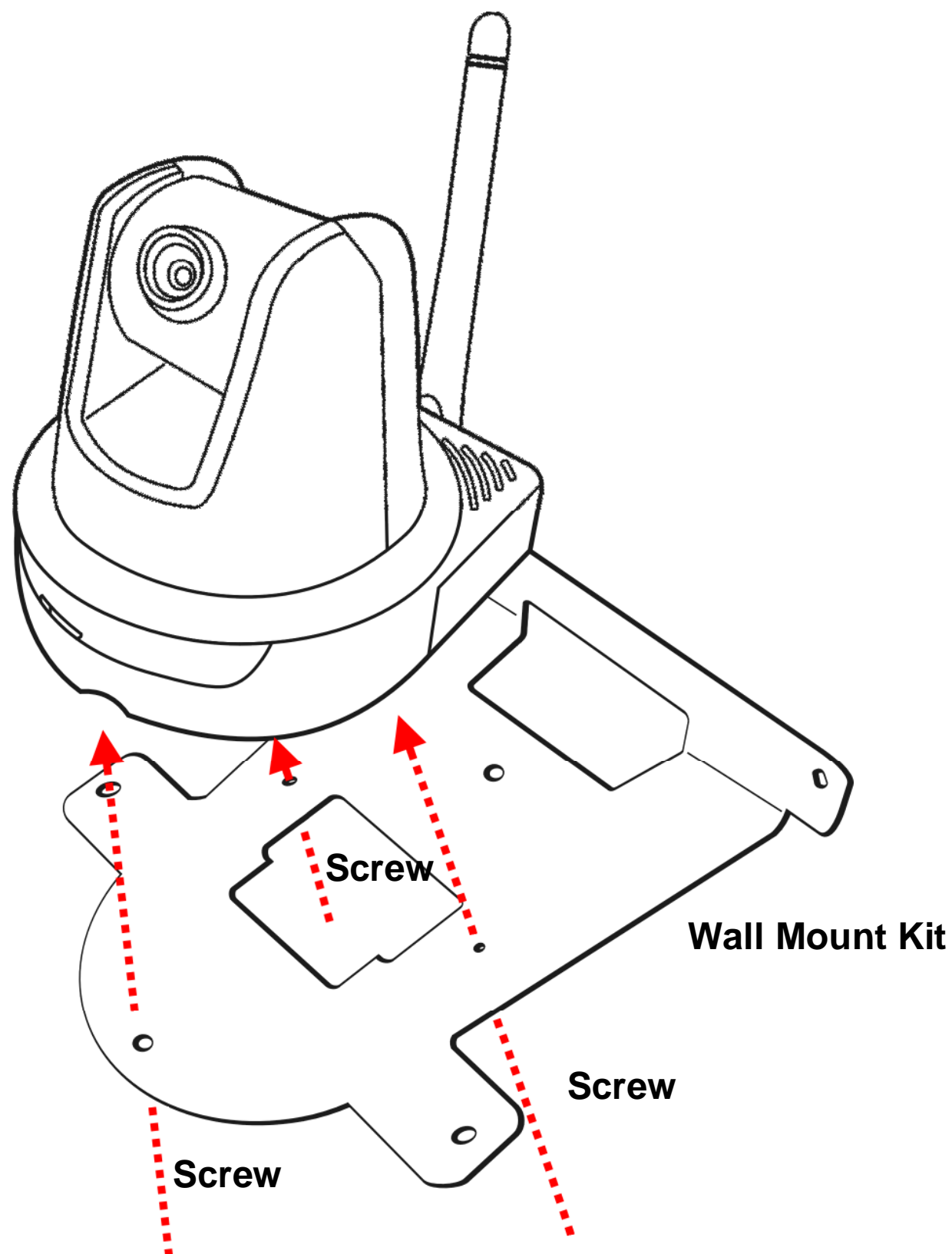
NOTE If you connect multiple cameras to monitor various places simultaneously, you are recommended to use a computer with higher performance.

CHAPTER 2

HARDWARE INSTALLATION

2.1 Installing the Wall Mount Kit

The camera comes with a Wall Mount Kit, which allows you to place your camera anywhere by mounting the camera through the three screw holes located in the base of the Wall Mount Kit.

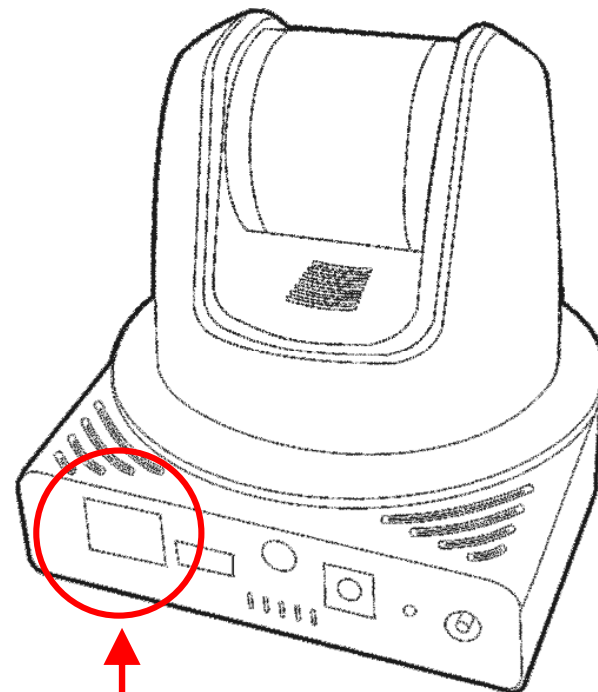


2.2 Connecting the Camera to LAN/WLAN

Use the provided Ethernet cable to connect the camera to your local area network (LAN).

When you connect the AC power adapter, the camera is powered on automatically. You can verify the power status from the Power LED on the front panel of the camera.

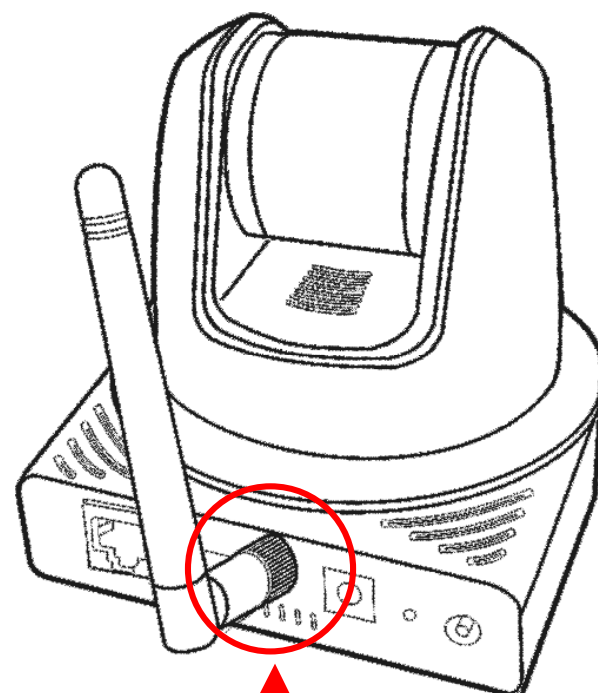
Once connected, the Link LED starts flashing green light and the camera is on standby and ready for use now.



Connecting the Ethernet Cable

If you use a wireless network in your application environment, you need to attach the included external antenna to the camera.

When the camera is powered on, the camera will automatically search any access point with “default” SSID.



Connecting the External Antenna

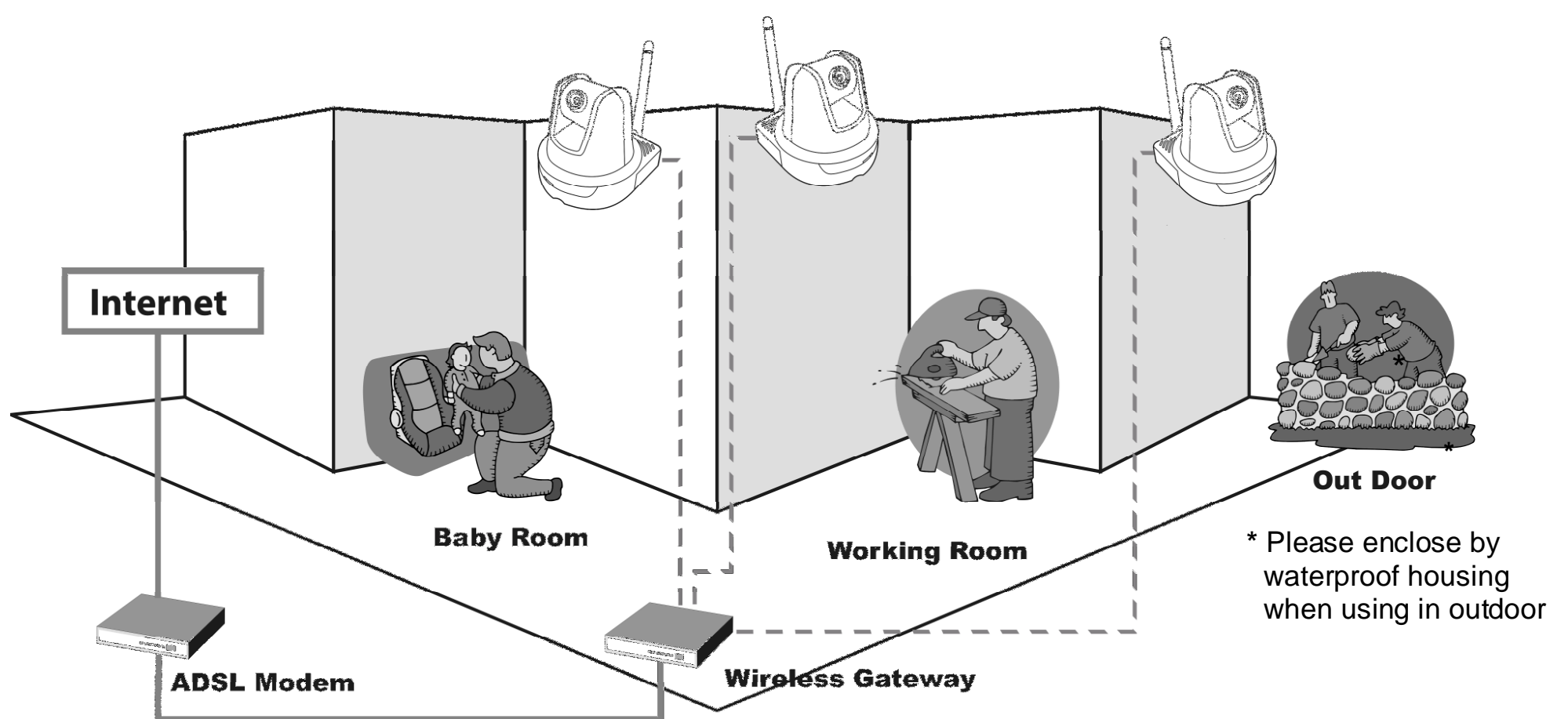
NOTE If the camera cannot connect to your wireless network, you need to install the camera in LAN and proceed with WLAN settings.

2.3 Applications of the Camera

The camera can be applied in multiple applications, including:

- Monitor local and remote places and objects via Internet or Intranet.
- Capture still images and video clips remotely.
- Upload images or send email messages with the still images attached.

The following diagram explains one of the typical applications for your camera and provides a basic example for installing the camera.



Home Applications

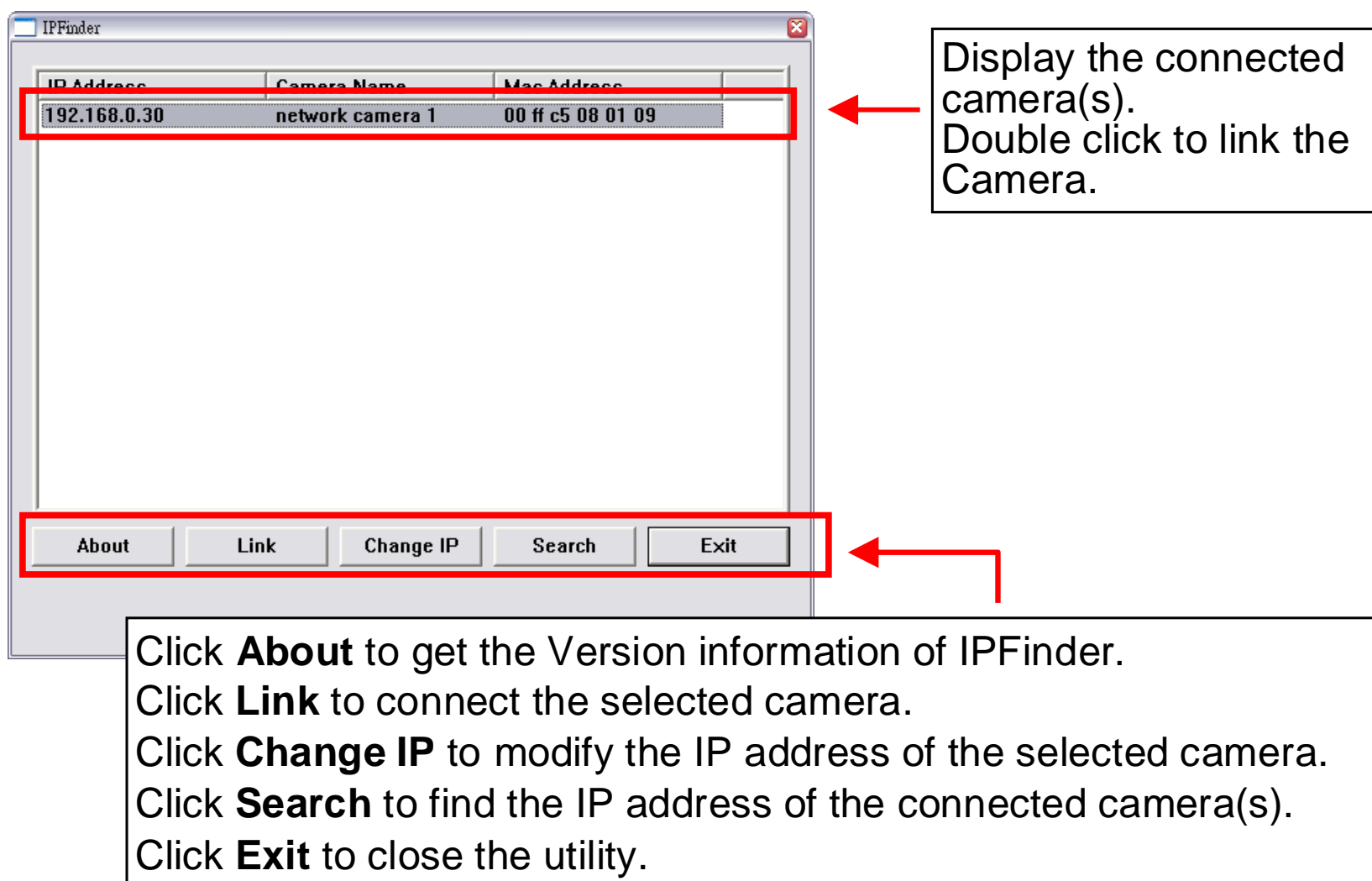
CHAPTER 3

ACCESSING THE CAMERA

3.1 Using IPFinder

The camera comes with a convenient utility, IPFinder, which is included in the Installation CD-ROM, allowing you to search the camera on your network easily.

1. Insert the Installation CD-ROM into your computer's CD-ROM drive to initiate the Auto-Run program.
2. Click the **IPFinder** item to launch the utility. The control panel will appear as below.

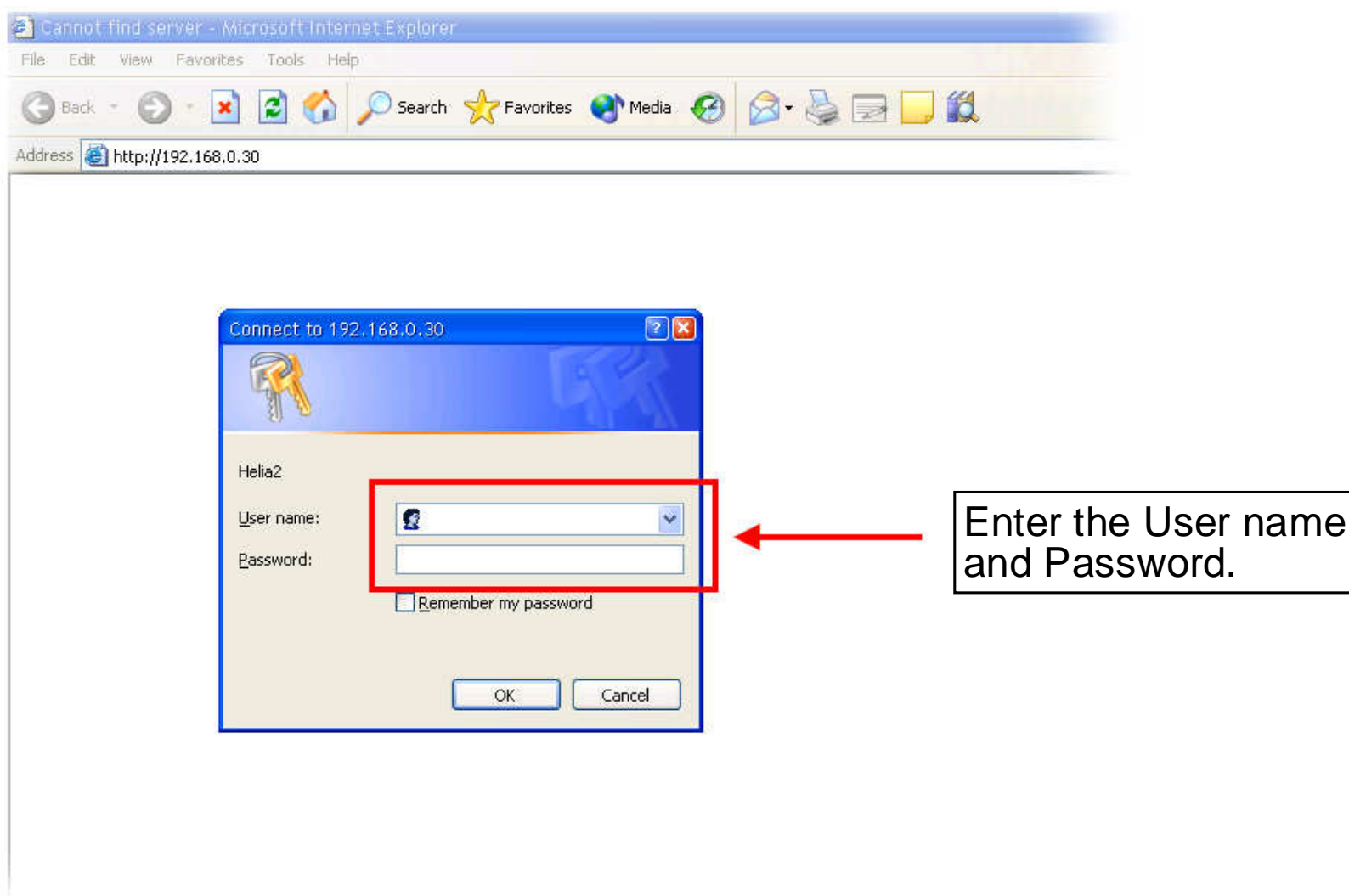


3. Once you get the IP address of the camera, launch the Web browser through the Link button or use UltraView software to access your camera.

3.2 Accessing to the Camera

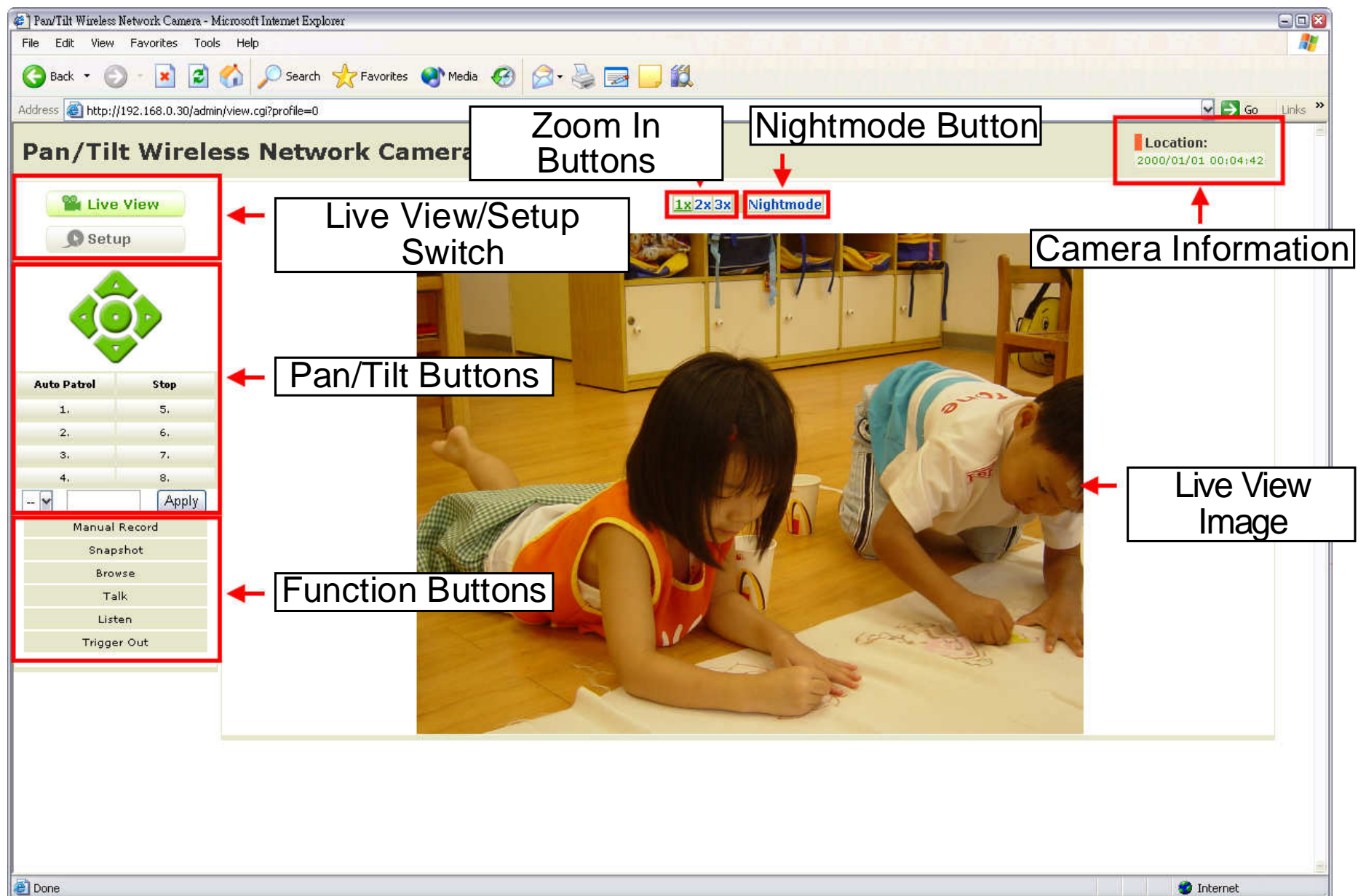
Whenever you want to access the camera:

1. Connect your camera to the network (or the PC directly).
2. Since the default configuration of the camera is DHCP mode enabled, you are recommended to launch IPFinder to search the IP address that is assigned to the camera by the DHCP server, and then click **Link** to access the camera via the Web browser.
3. When the login window appears, enter the default User name (**admin**) and password (**admin**) and press **OK** to access to the main screen of the camera's Web Configuration.



NOTE If you are initially access to the camera, you will be ask to install a new plug-in for the camera. Permission request depends on the Internet security settings of your computer. Click **Yes** to proceed.

After you login into the Web Configuration of the camera, the main page will appear as below:

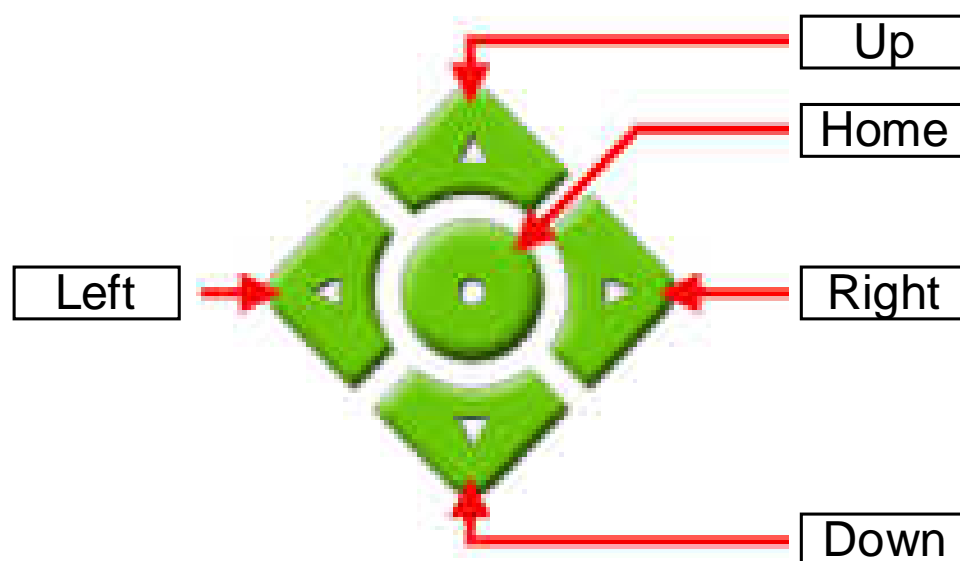


The main page of the Web Configuration provides you with many useful information and functions, including:

- **Camera Information** – Displays the camera's location and the current date & time. The information can be modified in the Web Configuration.
- **Live View Image** – Displays the real-time image of the connected camera.
 - Move your mouse to the Live View area and click on anywhere, the camera lens will then move to the position where you clicked to display it in the central part of Live View area.
 - When you enlarge the Live View by clicking the Zoom In buttons (2x or 3x), you can move the displayed image by right-clicking your mouse on the Live View area. The position

where you right-clicked will be displayed in the central part of Live View area.

- **Zoom In Buttons** – Click the buttons to zoom in the live view image by 1x, 2x, and 3x.
- **Nightmode Button** – Click the button to enable the “nightshot mode” to deliver clearer images in the dark environment. However, this will reduce the frame rate of video setting.
- **Live View/Setup Switch** – Click **Setup** to configure the camera. For details, see [Chapter 4](#).
- **Pan/Tilt Buttons** – Provides the buttons to control the camera lens:
 - **Left/Right/Up/Down/Home** buttons allow you to move the camera lens position. Clicking the **Home** button will move the camera lens to the assigned home position.



- **Auto Patrol** button controls the camera to automatically scan the preset positions once. Click **Stop** to stop patrolling.
- Click the **Number button** (1~8) to move the camera lens to the preset position immediately.

To set up the preset positions, move the camera lens by clicking the Left/Right/Up/Down buttons to the desired position first, then select the number (1~8) from the pull-down list and click the **Apply** button. You can enter a descriptive name for the assigned position in the text box to identify it easily.

- **Function Buttons** – Use these buttons to control the audio, video, and trigger functions.
 - **Manual Record** allows you to record and save a video clip.
 - **Snapshot** allows you to capture and save a still image.
 - **Browse** allows you to assign the destination folder to store the video clips and still images.
 - **Talk** allows you to speak out through the camera. Please note only one user is allowed to use this function at a time.
 - **Listen** allows you to receive the on-site sound and voice from the camera.
 - **Trigger Out** allows you to trigger on/off the GPIO output manually.

NOTE If your PC use Microsoft Vista platform, maybe you can't find these recorded files what stored by **Snapshot** or **Manual Record**. You need to disable the protected mode of Security in the IE Browser. Please follow as below Steps:

1. Open IE Browser
2. Select **Tools**→ **Internet Options**
3. Select **Security**
4. Disable the “**Enable Protected Mode**” then press **OK**

3.3 Configuring the IP Address of the PC

If you are failed to access to the camera, please check the IP address of your computer. When you connect the camera to your computer directly to proceed with configuration of the camera, you need to set up the IP addresses to be in the same segment for the two devices to communicate.

1. On your computer, click **Start > Control Panel** to open the Control Panel window.
2. Double-click **Network Connection** to open the Network Connection window.
3. Right-click **Local Area Connection** and then click **Properties** from the shortcut menu.
4. When the Local Area Connection Properties window appears, select the **General** tab.
5. Select **Internet Protocol [TCP/IP]** and then click **Properties** to bring up the Internet Protocol [TCP/IP] Properties window.
6. To configure a fixed IP address that is within the segment of the camera, select the **Use the following IP address** option. Then, enter an IP address into the empty field. The suggested IP address is **192.168.0.x** (x is 1~254 except 30), and the suggested Subnet mask is **255.255.255.0**.
7. When you finished the setting, click **OK**.

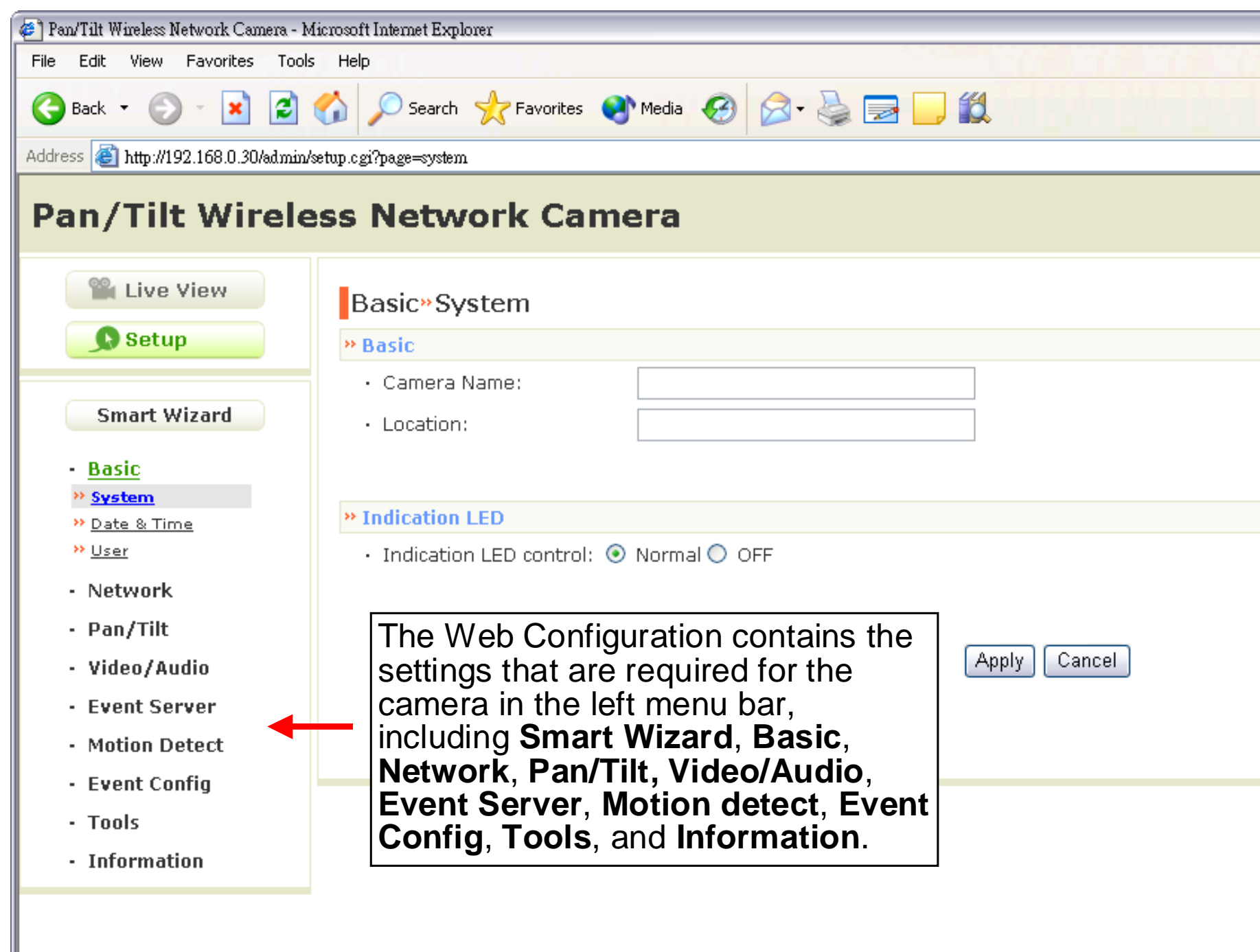
CHAPTER 4

CONFIGURING THE CAMERA

4.1 Using the Web Configuration

You can access and manage the camera through the Web browser and the provided software application UltraView. This chapter describes the Web Configuration, and guides you through the configuration of the camera by using the Web browser.

To configure the camera, click **Setup** on the main page of Web Configuration. The Web Configuration will start from the **Basic** page.



4.2 Using Smart Wizard

The camera’s Smart Wizard lets you configure your camera easily and quickly. The wizard will guide you through the necessary settings with detailed instructions on each step.

To start the wizard, click **Smart Wizard** in the left menu bar.

Step 1. Camera Settings

Camera Setting

• Camera Name:

network camera 1

• Location:

classroom 1

• Admin Password:

•••••

• Confirm Password:

•••••

Enter the name for the camera and place.

Enter the administrator password set.

Next >

Cancel

Step 2. IP Settings

IP Setting

☒ DHCP

☐ Static IP

• IP:

192 . 168 . 0 . 30

• Subnet Mask:

255 . 255 . 255 . 0

• Default Gateway:

192 . 168 . 0 . 1

• Primary DNS:

• Secondary DNS:

☐ PPPoE

• User Name:

• Password:

Select the IP setting according to your network:
DHCP, Static IP, or PPPoE.

< Prev

Next >

Cancel

Step 3. Email Settings

Email Setting

SMTP Server Address:

mail.com

Sender Email Address:

mymail@mail.com

Authentication Mode:

None

SMTP

Sender User Name:

mymail

Sender Password:

.....

Receiver #1 Email Address:

john@mail.com

Receiver #2 Email Address:

jay@mail.com

Enter the required information to be able to send email with image.

< Prev

Next >

Cancel

Step 4. Wireless Networking

Wireless Networking

Network ID(SSID):

default

Site Survey

Wireless Mode:

Infrastructure

Ad-Hoc

Channel:

6

Authentication:

Open

Encryption:

None

WEP

Format:

ASCII

HEX

Key Length:

64 bits

128 bits

WEP Key 1

WEP Key 2

WEP Key 3

WEP Key 4

Complete the required settings for wireless networking.

< Prev

Next >

Cancel

- 24 -

Step 5. Confirm Settings

Confirm Settings

• Camera Name:

network camera 1

• Location:

classroom 1

• IP MODE:

DHCP

• IP Address:

192.168.0.30

• Subnet Mask:

255.255.255.0

• Default Gateway:

192.168.0.1

• Primary DNS:

• Secondary DNS:

• SMTP Server Address:

mail.com

• Sender Email Address:

mymail@mail.com

• Authentication Mode:

SMTP

• Sender User Name:

mymail

• Receiver #1 Email Address:

john@mail.com

• Receiver #2 Email Address:

jay@mail.com

• ESSID:

default

• Connection:

Infrastructure

• Channel:

6

• Authentication:

Open

• Encryption:

None

< Prev

Apply

Cancel

This step shows the configuration of your camera. When you confirm the settings, click **Apply** to finish the wizard and reboot the camera. Otherwise, click **Prev** to go back to the previous step(s) and change the settings. Or, click **Cancel** to end the wizard and discard the changes.

4.3 Basic Setup

The Basic menu contains three sub-menus that provide the system settings for the camera, such as the Camera Name, Location, Date & Time, and User management.

Basic >> System



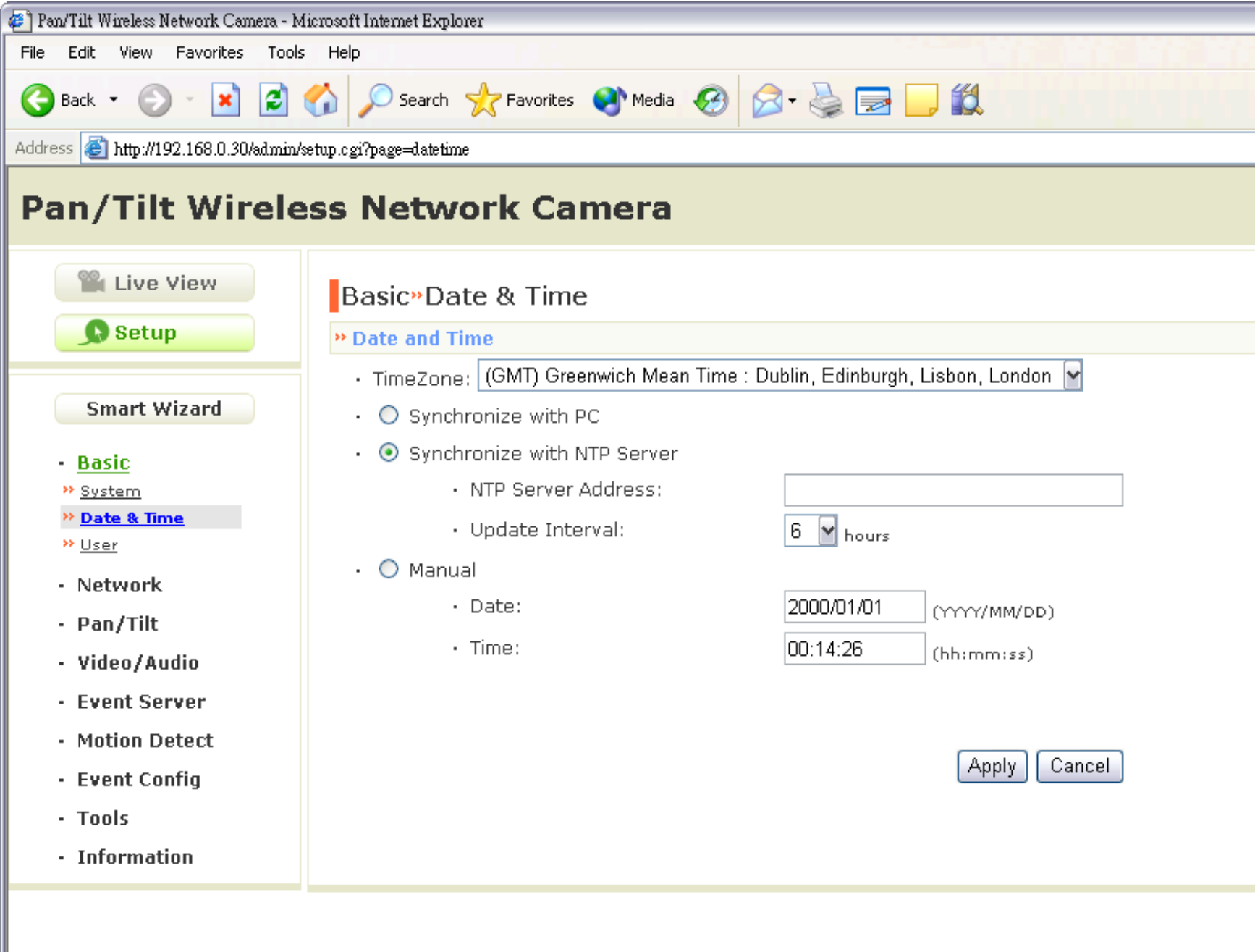
■ Basic

- **Camera Name:** Enter a descriptive name for the camera.
- **Location:** Enter a descriptive name for the location used by the camera.

■ Indication LED

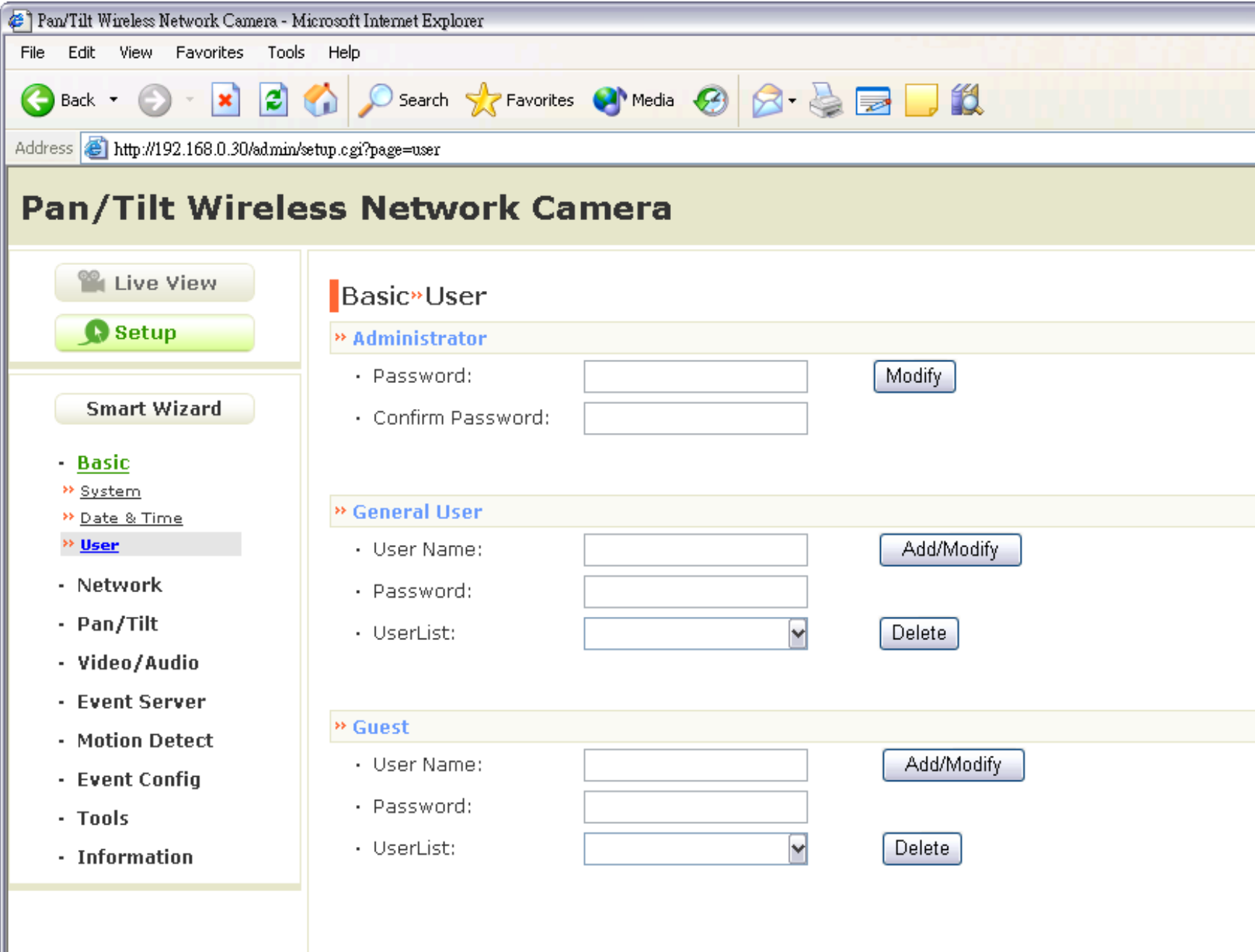
This item allows you to set the LED illumination as desired. There are two options: **Normal** and **OFF**.

Basic >> Date & Time



- **TimeZone:** Select the proper time zone for the region from the pull-down menu.
- **Synchronize with PC:** Select this option and the date & time settings of the camera will be synchronized with the connected computer.
- **Synchronize with NTP Server:** Select this option and the time will be synchronized with the NTP Server. You need to enter the IP address of the server and select the update interval in the following two boxes.
- **Manual:** Select this option to set the date and time manually.

Basic >> User



■ Administrator

To prevent unauthorized access to the camera’s Web Configuration, you are strongly recommended to change the default administrator password. Type the administrator password twice to confirm and set the password.

■ General User

- **User Name:** Enter the user’s name you want to add to use the camera.
- **Password:** Enter the password for the new user.

When you are finished, click **Add/Modify** to add the new user to the camera. To modify the user’s information, select the one you want to modify from **UserList** and click **Add/Modify**.

- **UserList:** Display the existing users of the camera. To delete a user, select the one you want to delete and click **Delete**.

■ Guest

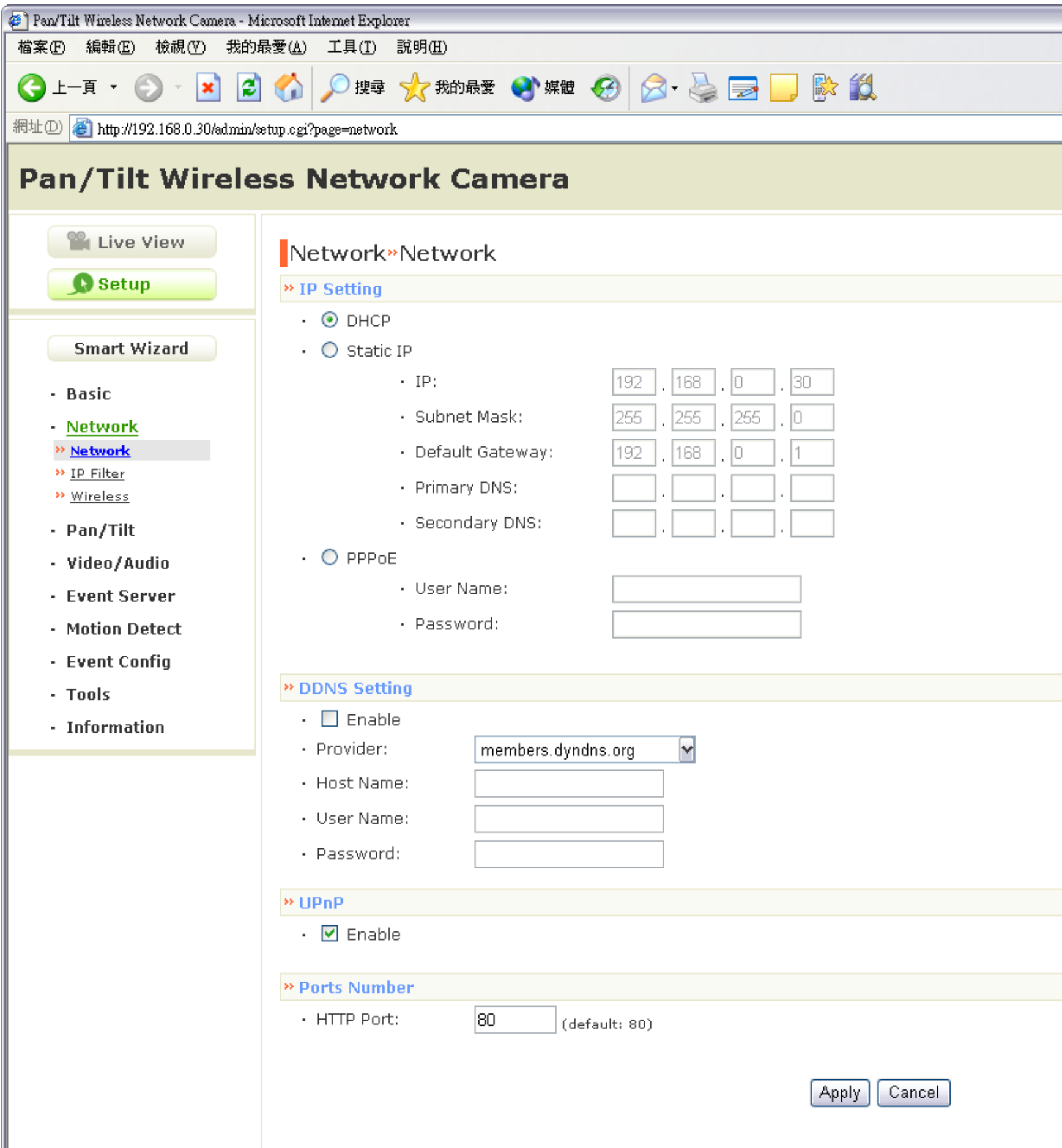
- **User Name:** Enter the guest's name you want to add to use the camera.
- **Password:** Enter the password for the new guest.
- **UserList:** Display the existing guests of the camera. To delete a user, select the one you want to delete and click **Delete**.

NOTE The “General User” can access the camera and control the Function buttons of the camera's Web Configuration. The “Guest” can only view the live view image from the main page of the Web Configuration while accessing the camera. Only the “Administrator” is allowed to configure the camera through the Web Configuration.

4.4 Network Settings

The Network menu contains three sub-menus that provide the network settings for the camera, such as the IP Setting, DDNS Setting, IP Filter, and Wireless network.

Network >> Network



■ IP Setting

This item allows you to select the IP address mode and set up the related configuration. The default setting is **DHCP** mode enabled.

- **DHCP:** Select this option when your network uses the DHCP server. When the camera starts up, it will be assigned an IP address from the DHCP server automatically.
- **Static IP:** Select this option to assign the IP address for the camera directly. You can use IPFinder to obtain the related setting values.

IP	Enter the IP address of the camera. The default setting is 192.168.0.30.
Subnet Mask	Enter the Subnet Mask of the camera. The default setting is 255.255.255.0.
Default Gateway	Enter the Default Gateway of the camera. The default setting is 192.168.0.1.
Primary/ Secondary DNS	The DNS (Domain Name System) translates domain names into IP addresses. Enter the Primary DNS and Secondary DNS that are provided by your ISP.

- **PPPoE:** Select this option when you use a direct connection via the ADSL modem. You should have a PPPoE account from your Internet service provider. Enter the **User Name** and **Password**. The camera will get an IP address from the ISP as starting up.

NOTE Once the camera get an IP address from the ISP as starting up, it automatically sends a notification email to you. Therefore, when you select PPPoE as your connecting type, you have to set up the email or DDNS configuration in advance.

■ **DDNS Setting**

With the Dynamic DNS feature, you can assign a fixed host and domain name to a dynamic Internet IP address. Select the **Enable** option to enable this feature. Then, select the DDNS Provider from the pull-down list and enter the required information in the **Host Name**, **User Name**, and **Password** boxes. Please note that you have to sign up for DDNS service with the service provider first.

■ **UPnP**

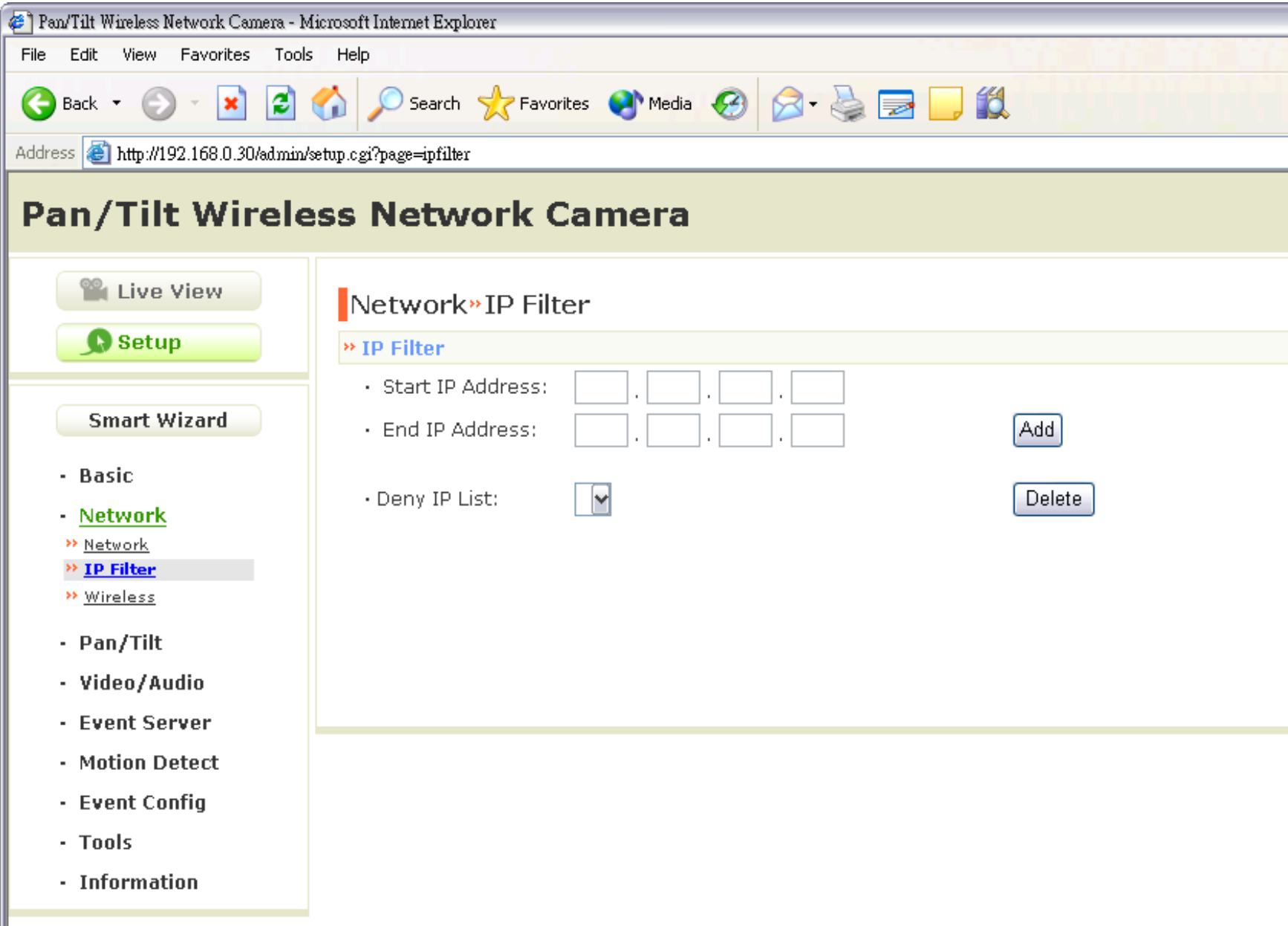
The camera supports UPnP (Universal Plug and Play), which is a set of computer network protocols that enable the device-to-device interoperability. In addition, it supports port auto mapping function so that you can access the camera if it is behind an NAT router or firewall. Select the **Enable** option to enable this feature.

■ **Ports Number**

- **HTTP Port:** The default HTTP port is **80**.

Network >> IP Filter

The IP Filter setting allows the administrator of the camera to limit the users within a certain range of IP addresses to access the camera.



■ Start/End IP Address

Assign a range of IP addresses that are not allowed to access the camera by entering the Start IP address and End IP address. When you finish the setting, click **Add** to save the range setting. You can repeat the action to assign multiple ranges for the camera.

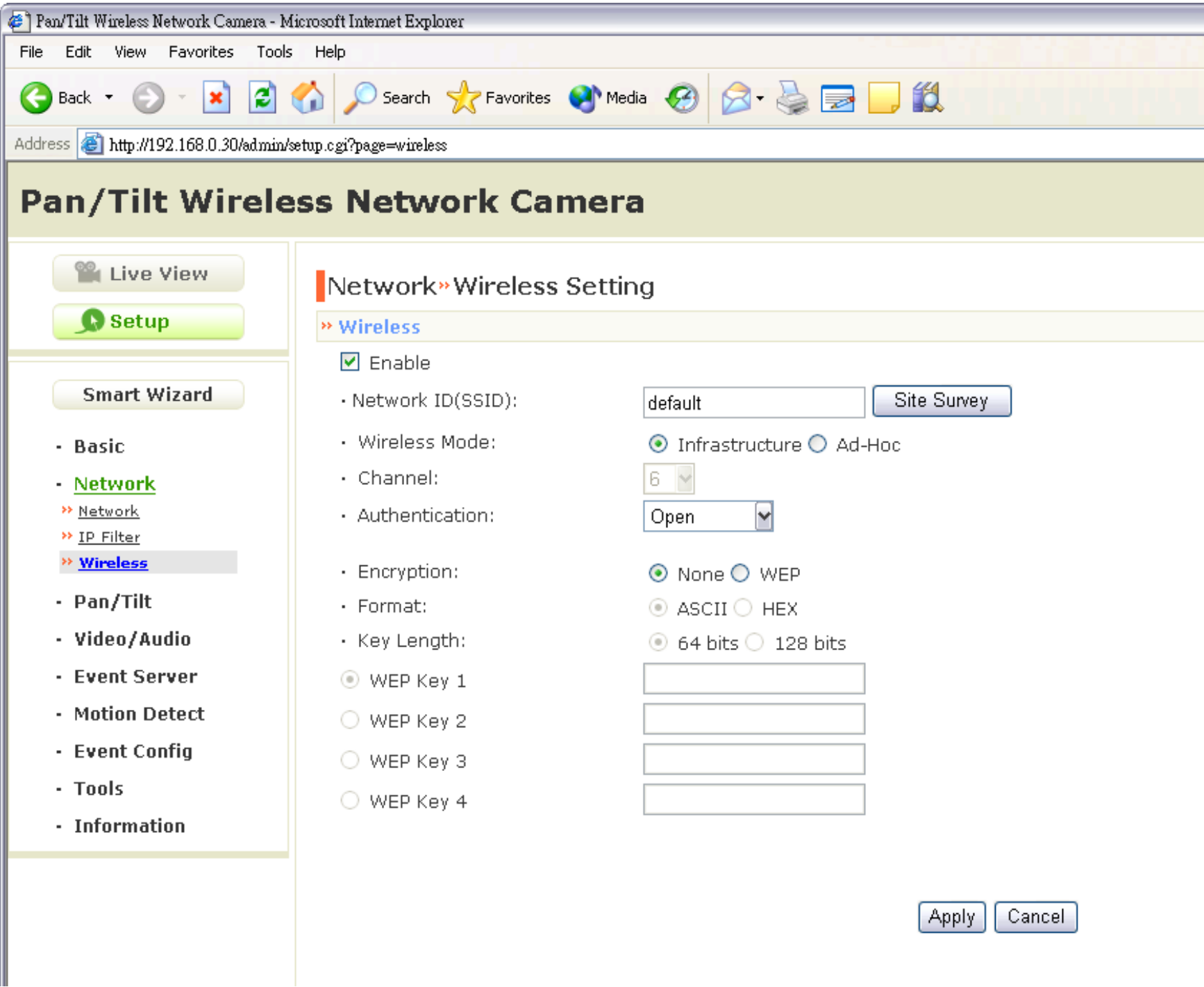
For example, when you enter 192.168.0.50 in Start IP Address and 192.168.0.80 in End IP Address, the user whose IP address located within 192.168.0.50 ~ 192.168.0.80 will not be allowed to access the camera.

■ **Deny IP List**

The list displays the range setting(s) of IP addresses that are not allowed to access the camera. To clear the setting, select a range of IP addresses from the list and click **Delete**.

Network >> Wireless Setting

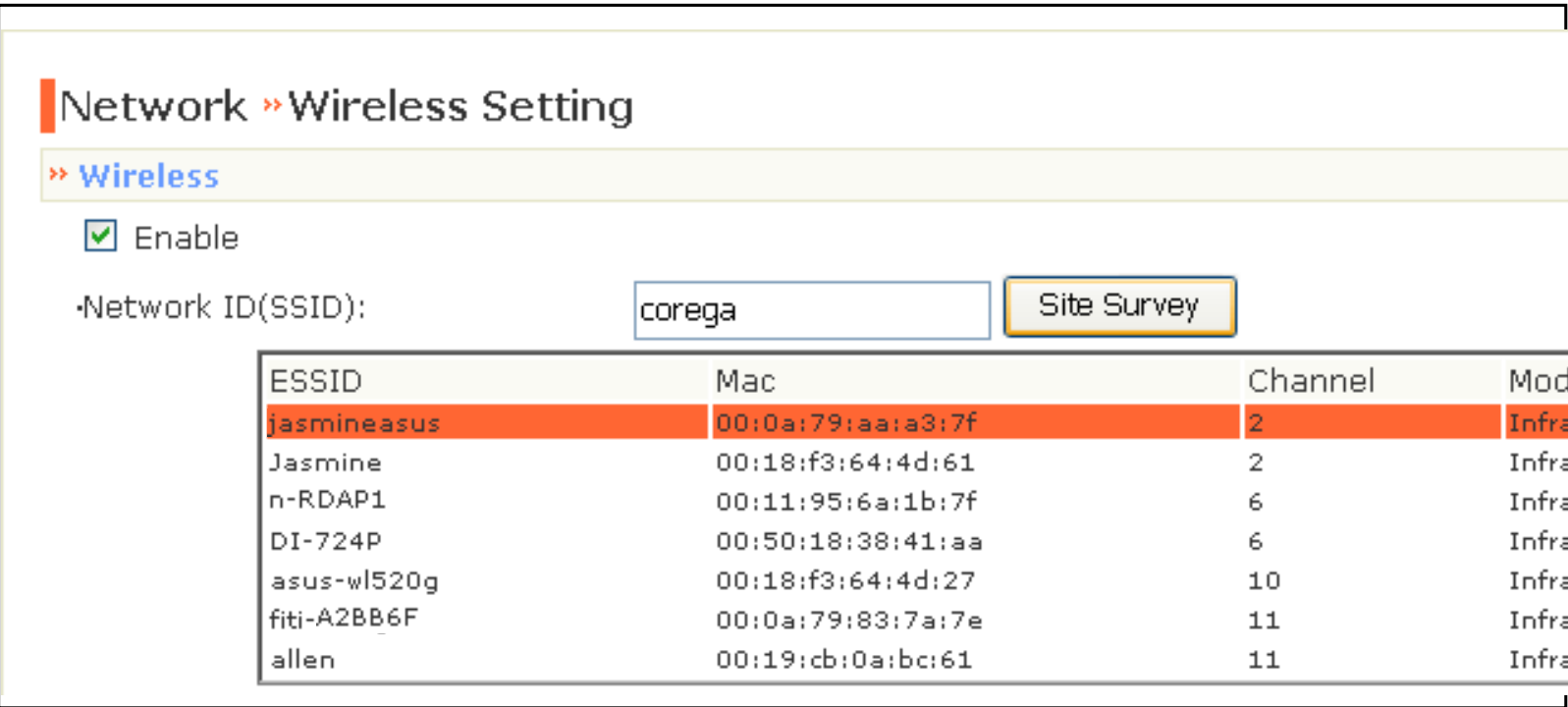
The camera supports WLAN while you use the wireless network. Select the **Enable** option to enable this feature.



- **Network ID (SSID):** Keep the default setting of this option to connect the camera to any access point under the infrastructure network mode. To connect the camera to a

specified access point, set a SSID for the camera to correspond with the access point’s ESS-ID. To connect the camera to an Ad-Hoc wireless workgroup, set the same wireless channel and SSID to match with the computer’s configuration.

Click **Site Survey** to display the available wireless networks, so that you can easily connect to one of the listed wireless networks.



List of searching results

- **Wireless Mode:** Select the type of wireless communication for the camera: **Infrastructure** or **Ad-Hoc**.
- **Channel:** Select the appropriate channel from the list.
- **Authentication:** Select the authentication method to secure the camera from being used by unauthorized user: **Open**, **Shared-key**, **WPA-PSK**, and **WPA2-PSK**. The following table explains the four options:

Open	The default setting of Authentication mode, which communicates the key across the network.
Shared-key	Allow communication only with other devices with identical WEP settings.
WPA-PSK/ WPA2-PSK	WPA-PSK/WPA2-PSK is specially designed for the users who do not have access to network

	authentication servers. The user has to manually enter the starting password in their access point or gateway, as well as in each PC on the wireless network.
--	---

If you select **Open** or **Shared-key** as the Authentication mode, you need to complete the following settings:

Encryption: Select the **WEP** option to enable the data encryption feature to secure the camera within the wireless network.

Format: Once you enable the Encryption feature, you need to determine the encryption format by selecting **ASCII** or **HEX**. ASCII format causes each character you type to be interpreted as an eight-bit value. Hex format causes each pair of characters you type to be interpreted as an eight-bit value in hexadecimal (base 16) notation.

Key Length: Select the WEP key length you want to use: **64 bits** or **128 bits**.

WEP Key 1/2/3/4: Enter the WEP key(s) in the following boxes.

If you select **WPA-PSK** or **WPA2-PSK** as the Authentication mode, you need to complete the following settings:

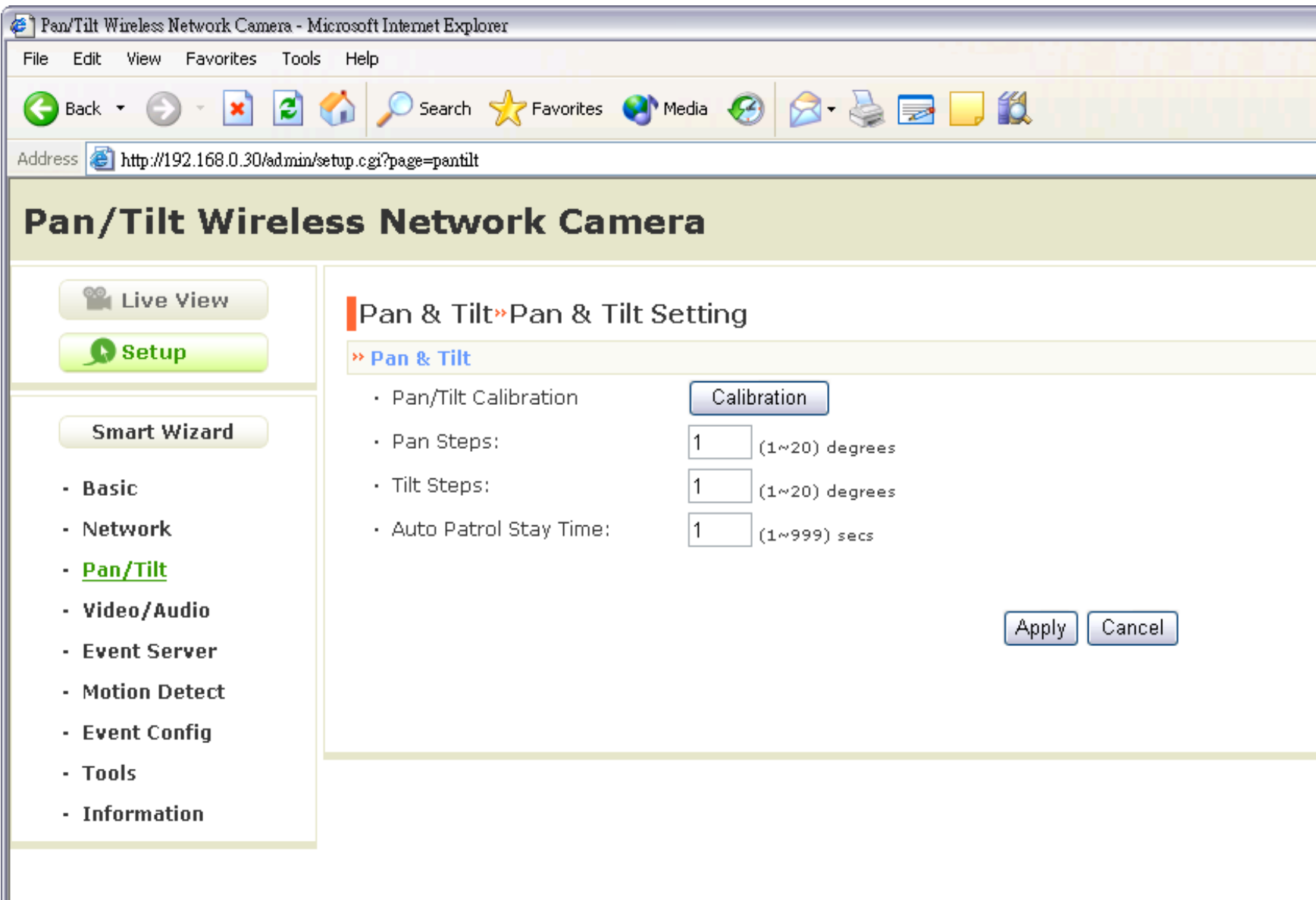
Encryption: Select **TKIP** or **AES**. TKIP (Temporal Key Integrity Protocol) changes the temporal key every 10,000 packets to insure much greater security than the standard WEP security. AES (Advanced Encryption Standard) is used to ensure the highest degree of security and authenticity for digital information.

Pre-Shared Key: This is used to identify each other in the network. Enter the name in the box, and this name must match the Pre-shared key value in the remote device.

4.5 Pan/Tilt Settings

The Pan/Tilt menu allows you to configure the pan/tilt functions of the camera.

Pan/Tilt >> Pan & Tilt Settings



- **Pan/Tilt Calibration:** Click **Calibration** to calibrate the position of the camera lens.
- **Pan Steps:** Set the changing range (1~20 degrees) when you click the Left/Right button.
- **Tilt Steps:** Set the changing range (1~20 degrees) when you click the Up/Down button.
- **Auto Patrol Stay Time:** Set the stay time (1~999 seconds) of each preset positions when the camera is patrolling.

4.6 Setting up Video & Audio

The Video & Audio menu contains three sub-menus that provide the video and audio settings for the camera.

Video & Audio >> Camera



■ Image Setting

- **Brightness:** Adjust the brightness level from 0 ~ 100.
- **Contrast:** Adjust the contrast level from 0 ~ 100.
- **Saturation:** Adjust the colors level from 0 ~ 100.

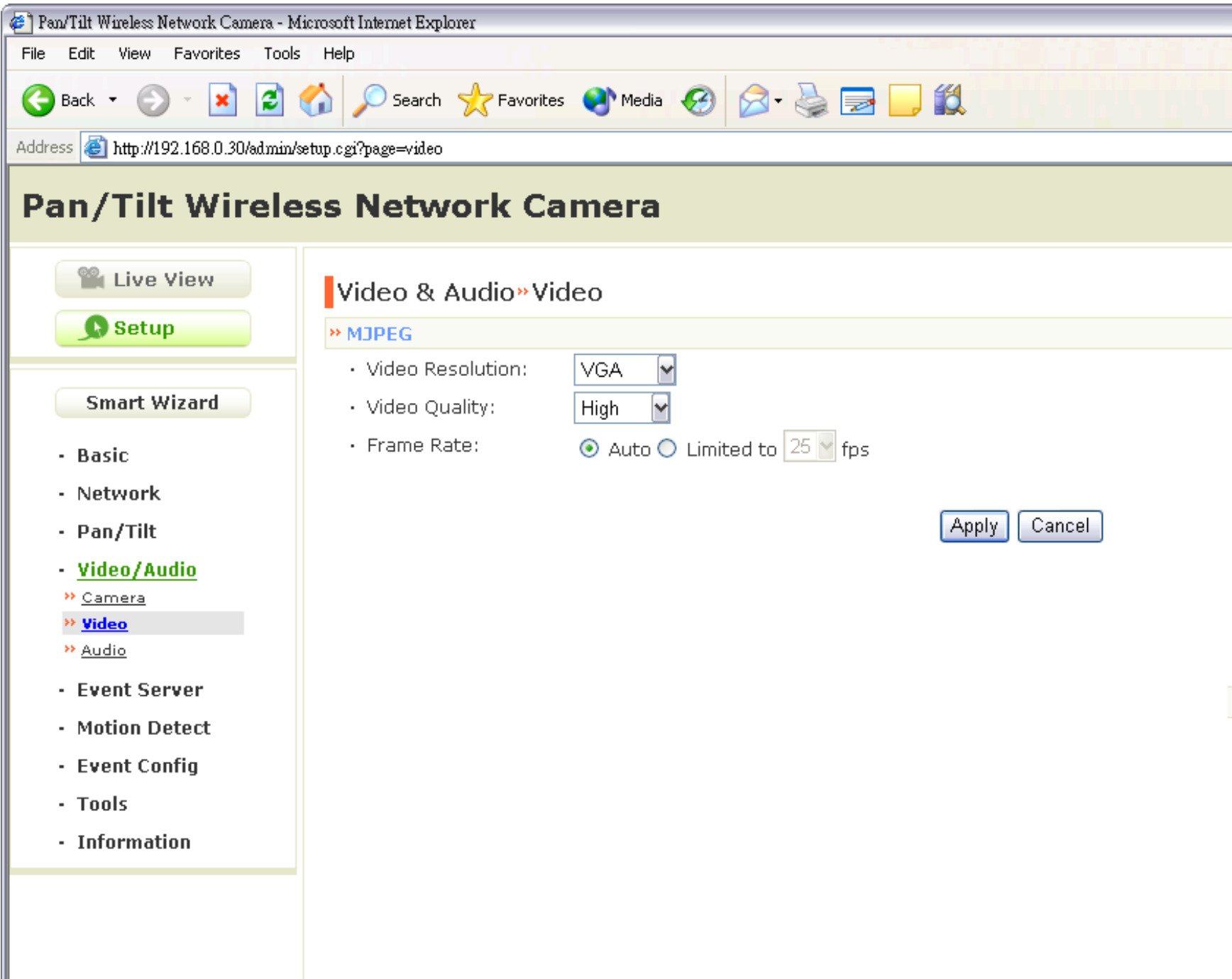
Click **Default** to restore the default settings of the three options above.

- **Mirror:** Select the **Horizontal** option to mirror the image horizontally. Select the **Vertical** option to mirror the image vertically.
- **Light Frequency:** Select the proper power frequency according to the camera's location: **50Hz**, **60Hz**, or **Outdoor**.

■ **Overlay Setting**

- **Includes Date & Time:** Select this option to display the date & time stamp on the live view image.
- **Enable Opaque:** Select this option to set a black background to the displayed date & time stamp.

Video & Audio >> Video



■ MJPEG

- **Video Resolution:** Select the desired video resolution from the three formats: **VGA**, **QVGA** and **QQVGA**. The higher setting (VGA) obtains better video quality while it uses more resource within your network.
- **Video Quality:** Select the desired image quality from five levels: **Lowest**, **Low**, **Medium**, **High**, and **Highest**.
- **Frame Rate:** Select **Auto** or a proper setting depending on your network status.

Video & Audio >> Audio



■ Camera Microphone In

Select the **Enable** option to enable the camera’s audio function, so that you can receive the on-site sound and voice from the camera.

■ Camera Speaker Out

Select the **Enable** option to enable the camera’s external speaker function, so that the connected speaker can play the sound and voice through the camera.

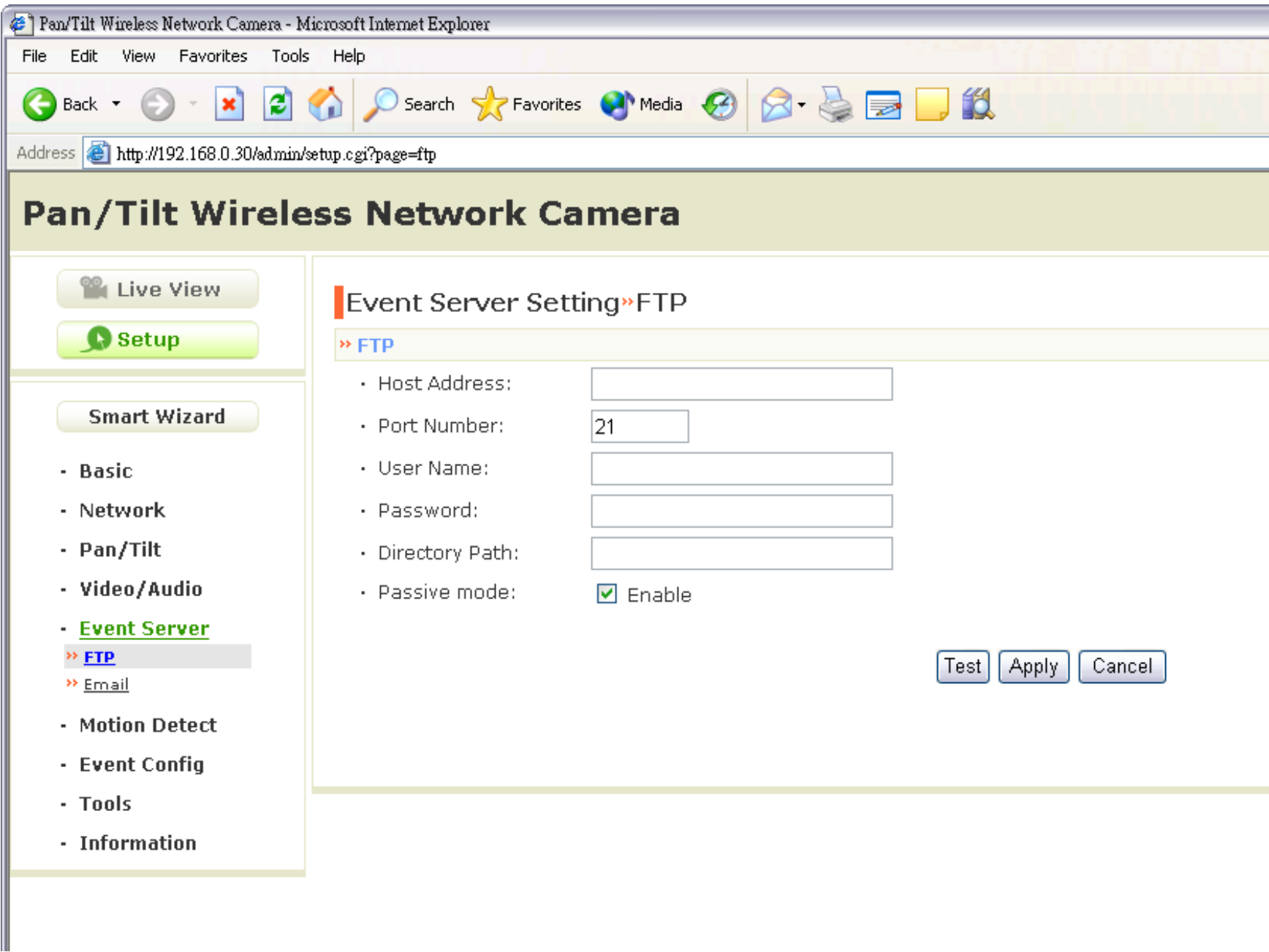
- **Volume:** Set the speaker’s volume.

4.7 Event Server Configuration

The Event Server menu contains two sub-menus that allow you to upload images to FTP, send emails that include still images, and store the images to a NAS system.

When you complete the required settings for FTP or Email, click **Test** to test the related configuration is correct or not. Once the camera connects to the server successfully, click **Apply**.

Event Server Setting>> FTP



- **Host Address:** Enter the IP address of the target FTP server.
- **Port Number:** Enter the port number used for the FTP server.
- **User Name:** Enter the user name to login into the FTP server.
- **Password:** Enter the password to login into the FTP server.

- **Directory Path:** Enter the destination folder for uploading the images. For example, /Test/.
- **Passive Mode:** Select the **Enable** option to enable passive mode.

Event Server Setting >> Email

The screenshot shows a web browser window titled "Pan/Tilt Wireless Network Camera - Microsoft Internet Explorer". The address bar shows "http://192.168.0.30/admin/setup.cgi?page=email". The page has a header "Pan/Tilt Wireless Network Camera" and a left sidebar with navigation links: "Live View", "Setup", "Smart Wizard", "Basic", "Network", "Pan/Tilt", "Video/Audio", "Event Server" (highlighted), "FTP", "Email" (highlighted), "Motion Detect", "Event Config", "Tools", and "Information". The main content area is titled "Event Server Setting >> Email" and contains the following fields:

- SMTP Server Address: mail.com
- Sender Email Address: mymail@mail.com
- Authentication Mode: ☐ None ☒ SMTP
- Sender User Name: mymail
- Sender Password: [Redacted]
- Receiver #1 Email Address: john@mail.com
- Receiver #2 Email Address: jay@mail.com

At the bottom right of the form are three buttons: "Test", "Apply", and "Cancel".

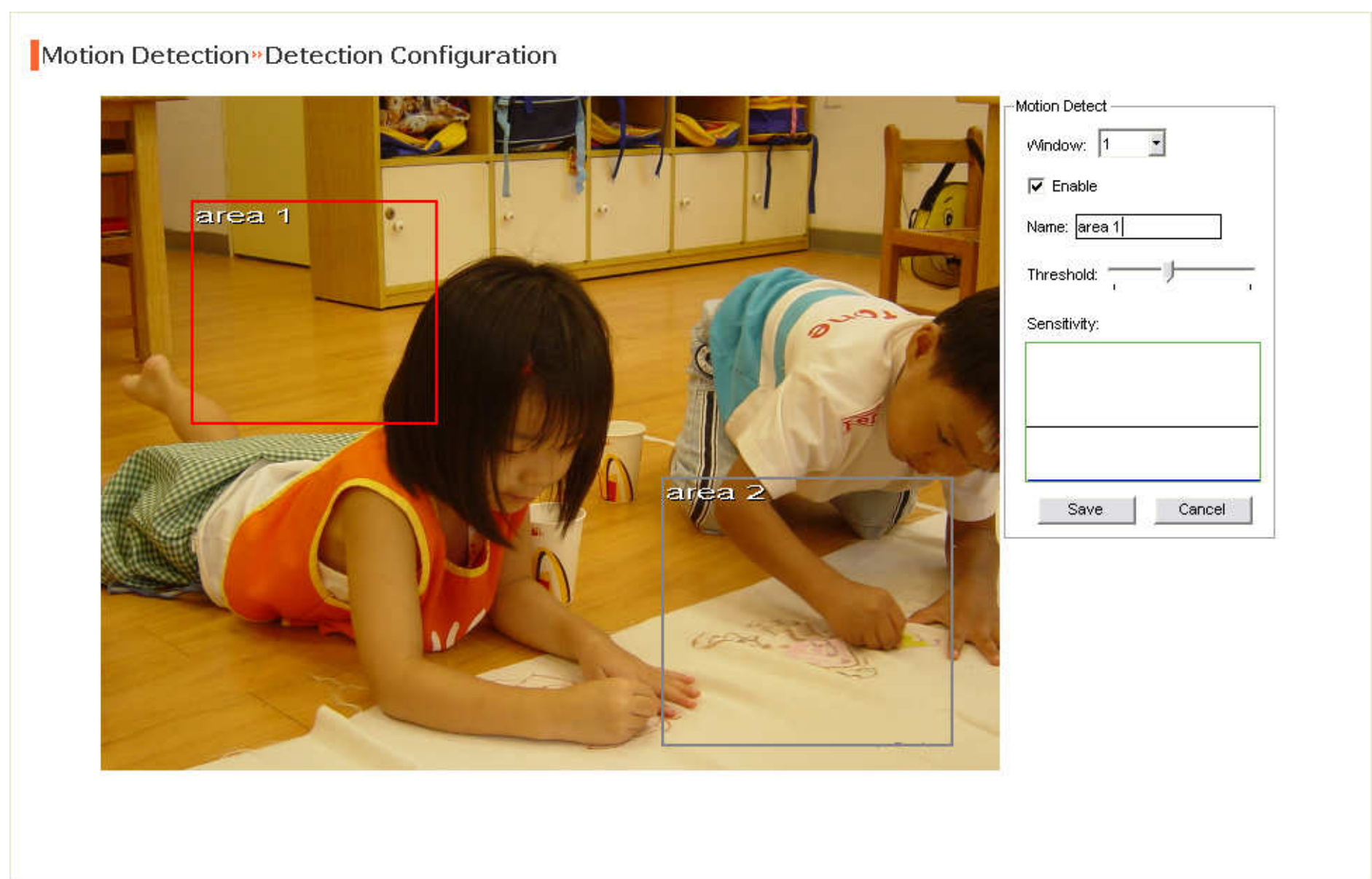
- **SMTP Server Address:** Enter the mail server address. For example, mymail.com.
- **Sender Email Address:** Enter the email address of the user who will send the email. For example, John@mymail.com.
- **Sender User Name:** Enter the user name to login the mail server.

- **Sender Password:** Enter the password to login the mail server.
- **Receiver #1 Email Address:** Enter the first email address of the user who will receive the email.
- **Receiver #2 Email Address:** Enter the second email address of the user who will receive the email.

4.8 Motion Detect

The Motion Detect menu contains the command and option that allow you to enable and set up the motion detection feature of the camera. The camera provides two detecting areas.

To enable the detecting area, select **Window 1** or **2** from the pull-down list, and then select **Enable**. When the detecting area is enabled, you can use the mouse to move the detecting area and change the area coverage.



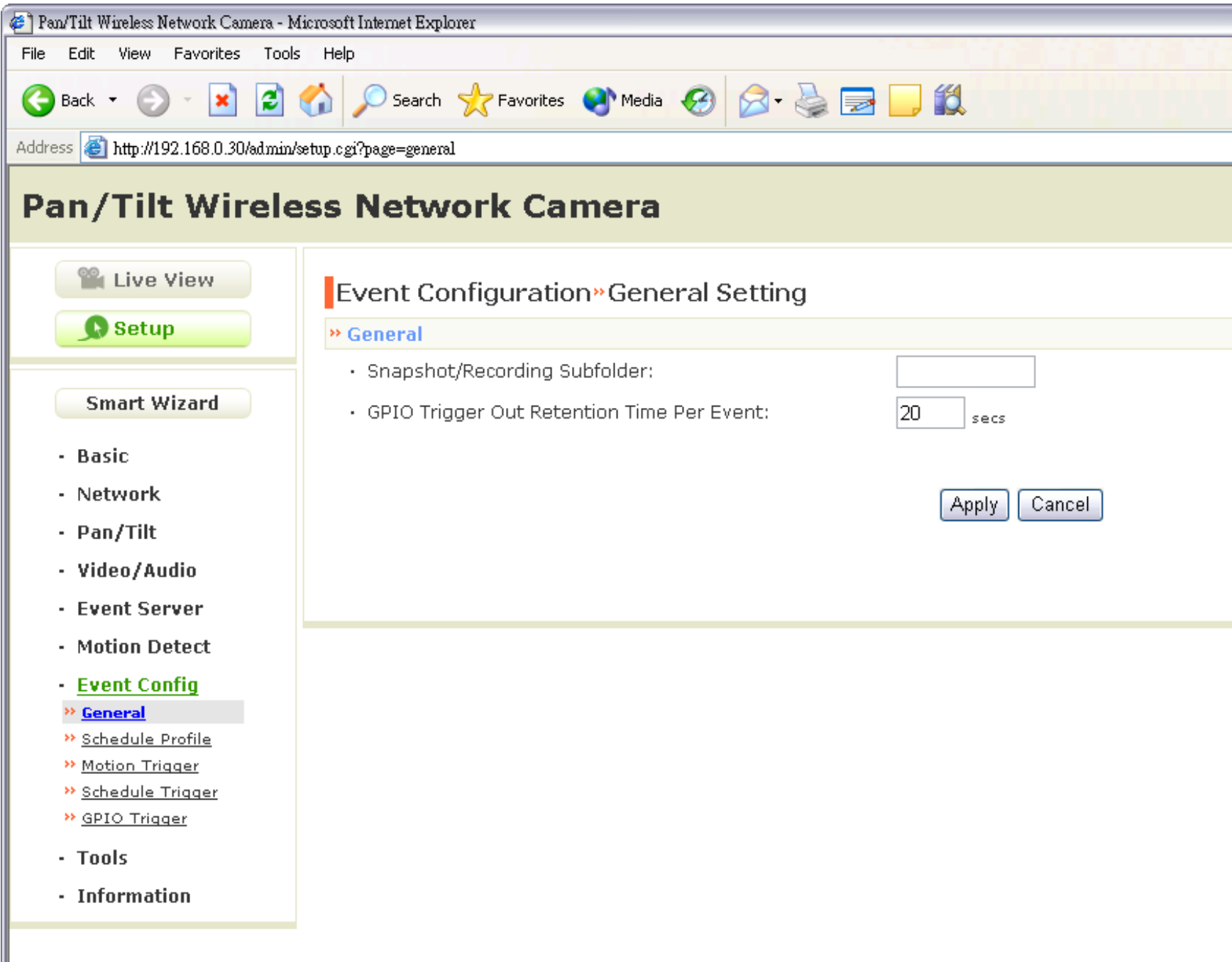
- **Name:** Assign a name to the detecting area.
- **Threshold:** Move the slide bar to adjust the level for detecting motion to record video.

NOTE Sliding the Threshold bar to the right will decrease the sensitivity of motion detection; sliding the Threshold bar to the left will increase the sensitivity of motion detection

4.9 Event Config

The Event Config menu contains five sub-menus that provide the commands to configure event profiles.

Event Configuration >> General Setting



- **Snapshot/Recording Subfolder:** You can assign a descriptive name for the subfolder to save the captured image/video files. Otherwise, leave this option blank to use the default setting.
- **GPIO Trigger Out Retention Time Per Event:** Limit the retention time of the GPIO Trigger Out function.

Event Configuration >> Arrange Schedule Profile

This sub-menu displays the scheduled profile(s). To customize the profile, click **Add** and then enter a descriptive name for the profile in the prompt dialog window. After entering the profile name, click **OK** and the profile is added to the Schedule Profiles list. To delete the profile, select the profile in the list and click **Delete**.

Event Configuration>>Arrange Schedule Profile

>> Schedule Profiles

classroom1

Add

Delete

•Profile Name:

classroom1

•Weekdays:

☐ Sun

☒ Mon

☐ Tue

☐ Wed

☐ Thr

☐ Fri

☐ Sat

•Time List:

09:00 - 12:00

13:00 - 17:00

Add

Add this to all weekdays

Delete

Delete this from all weekdays

•Start Time:

13

:

00

•End Time:

17

:

00

Save

- **Profile Name:** Display the profile name that you select in the Schedule Profiles list.
- **Weekdays:** Select the weekday(s) that you want to separately assign in the schedule profile. The weekday that has been assigned will be displayed with green color.
- **Time List:** Display the time period that you have assigned within the selected weekday. To assign the same time period to every weekday, click **Add this to all weekdays**; click **Delete this from all weekdays** to remove the selected time period from every weekday. Click Delete to remove the selected time period.
- **Start/End Time:** Enter the start and end time and then click **Add** to assign a time period within in the selected weekday.

Event Configuration >> Motion Detect Trigger

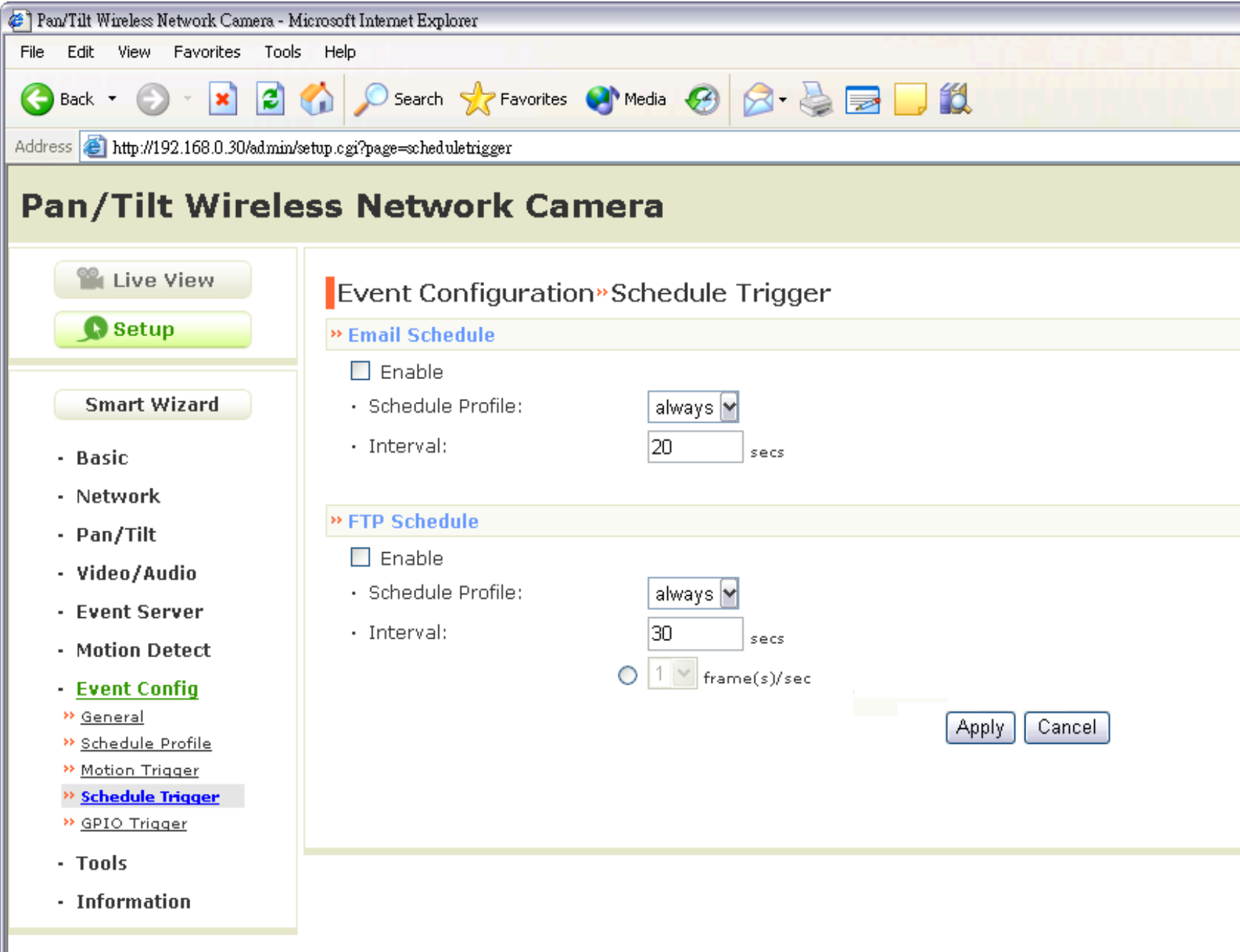
Select the **Enable** option to enable the motion detect trigger function of the camera, so that you can set Trigger Out function or send captured images within the detecting area to the FTP server or email receiver. You have to configure corresponding settings, such as FTP server and email server, to enable this feature.



- **Schedule Profile:** Select a schedule profile from the pull-down list.
- **Action:** Set the **Trigger Out** function or select the destination of the captured images: **Send Email** or **FTP Upload**.

Event Configuration >> Schedule Trigger

You can separately configure the schedule for trigger function of the camera by **Email** or **FTP**. Select the **Enable** option on each item, and then select a **Schedule Profile** from the pull-down list and set the **Interval** time.

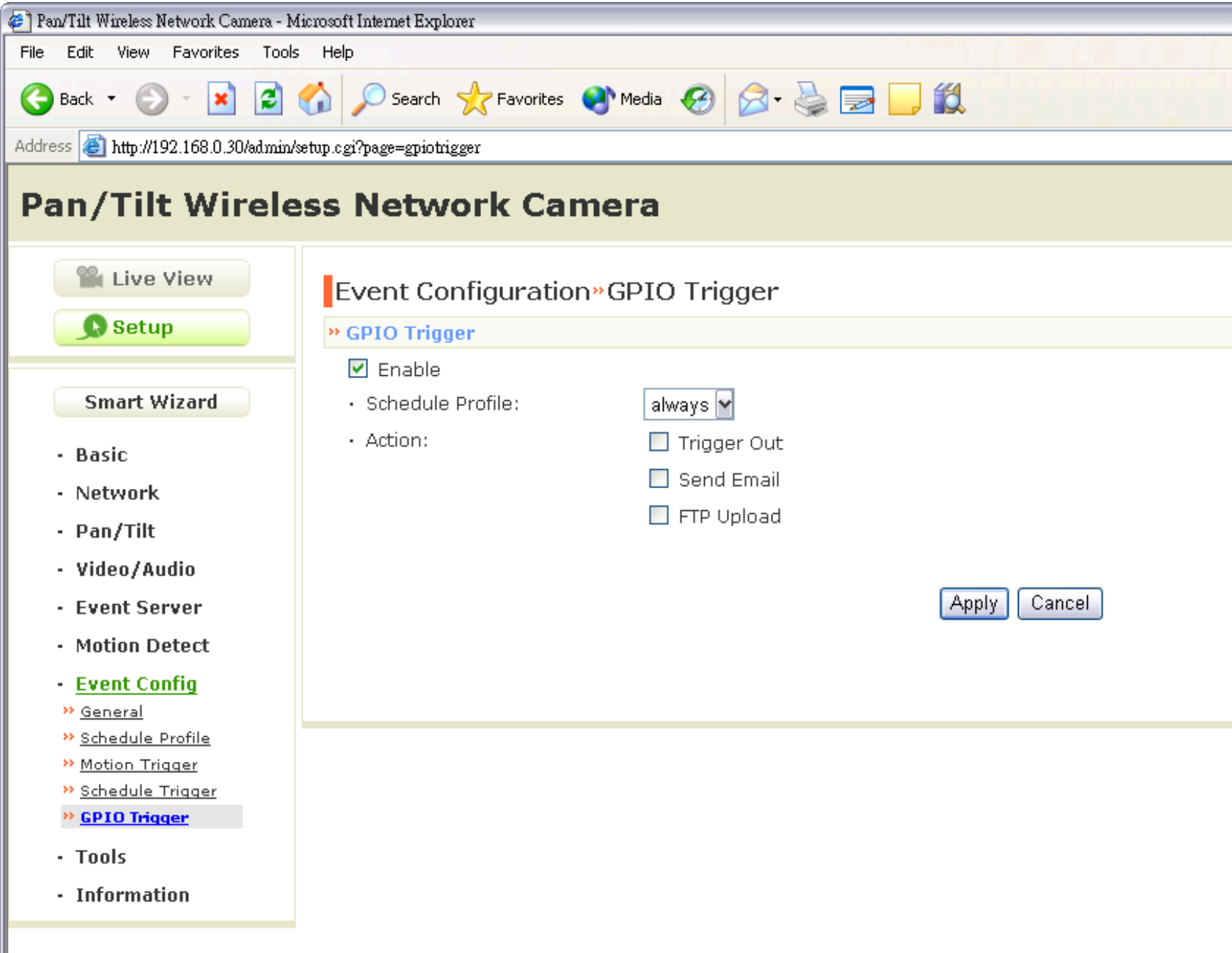


Email/FTP Schedule

- **Schedule Profile:** Select a schedule profile from the pull-down list.
- **Interval:** Enter a number in this box to setup the time (in second) to send Email or upload to FTP regularly.

Event Configuration >> GPIO Trigger

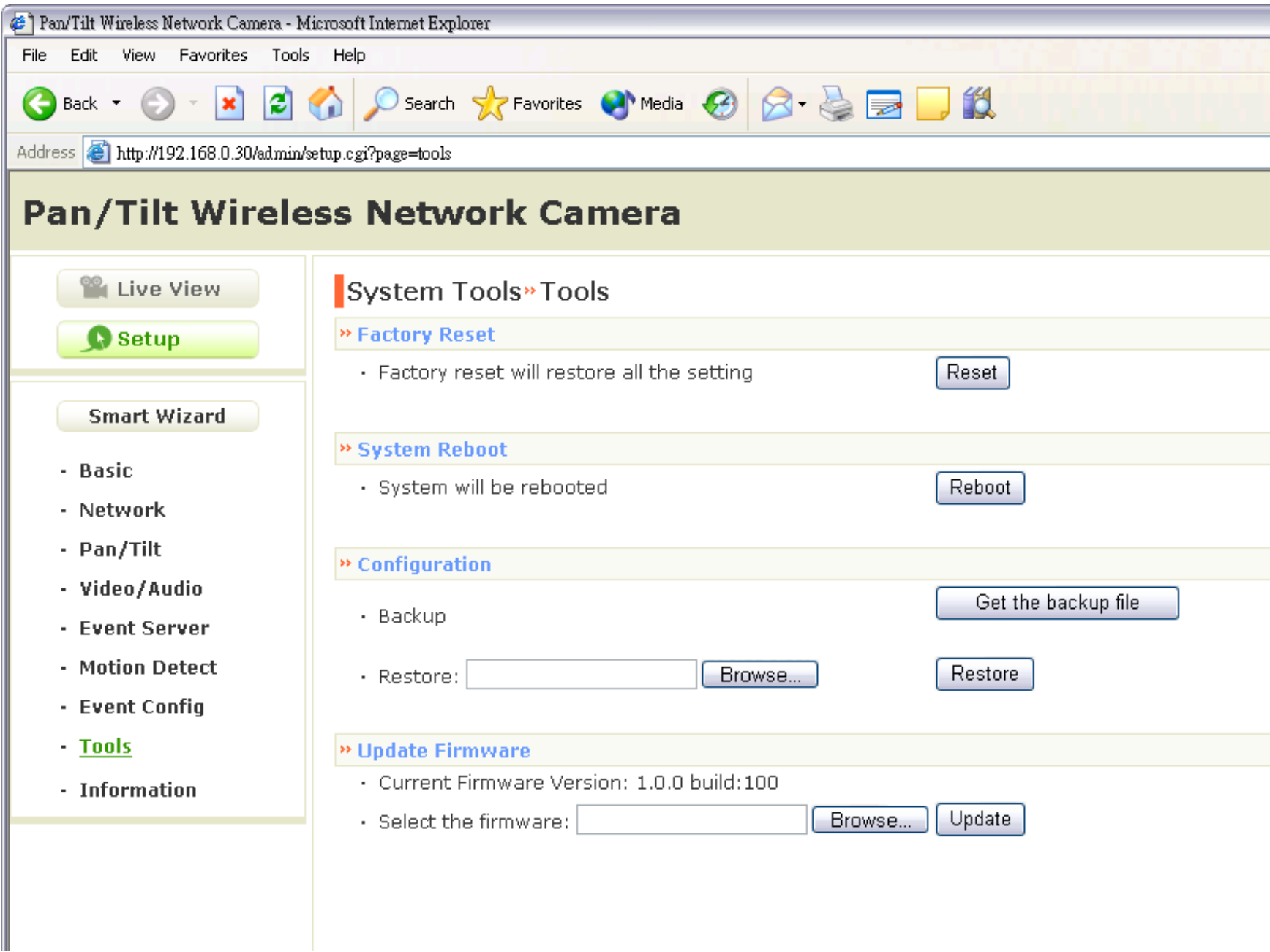
Select the **Enable** option to enable the GPIO trigger function of the camera, so that you can set Trigger Out function or send captured images within the detecting area to the FTP server or email receiver. You have to configure corresponding settings, such as FTP server and email server, to enable this feature.



- **Schedule Profile:** Select a schedule profile from the pull-down list.
- **Action:** Set the **Trigger Out** function or select the destination of the captured images: **Send Email** or **FTP Upload**.

4.10 Tools

The Tools menu provides the commands that allow you to restart or reset the camera. You can also backup and restore your configuration, and upgrade the firmware for the camera.



■ Factory Reset

Click **Reset** to restore all factory default settings for the camera.

■ System Reboot

Click **Reboot** to restart the camera just like turning the device off and on. The camera configuration will be retained after rebooting.

■ Configuration

You can save your camera configuration as a backup file on your computer. Whenever you want to resume the original settings, you can restore them by retrieving the backup file.

- **Backup:** Click **Get the backup file** to save the current configuration of the camera.
- **Restore:** Click **Browse** to locate the backup file and then click **Restore**.

■ **Update Firmware**

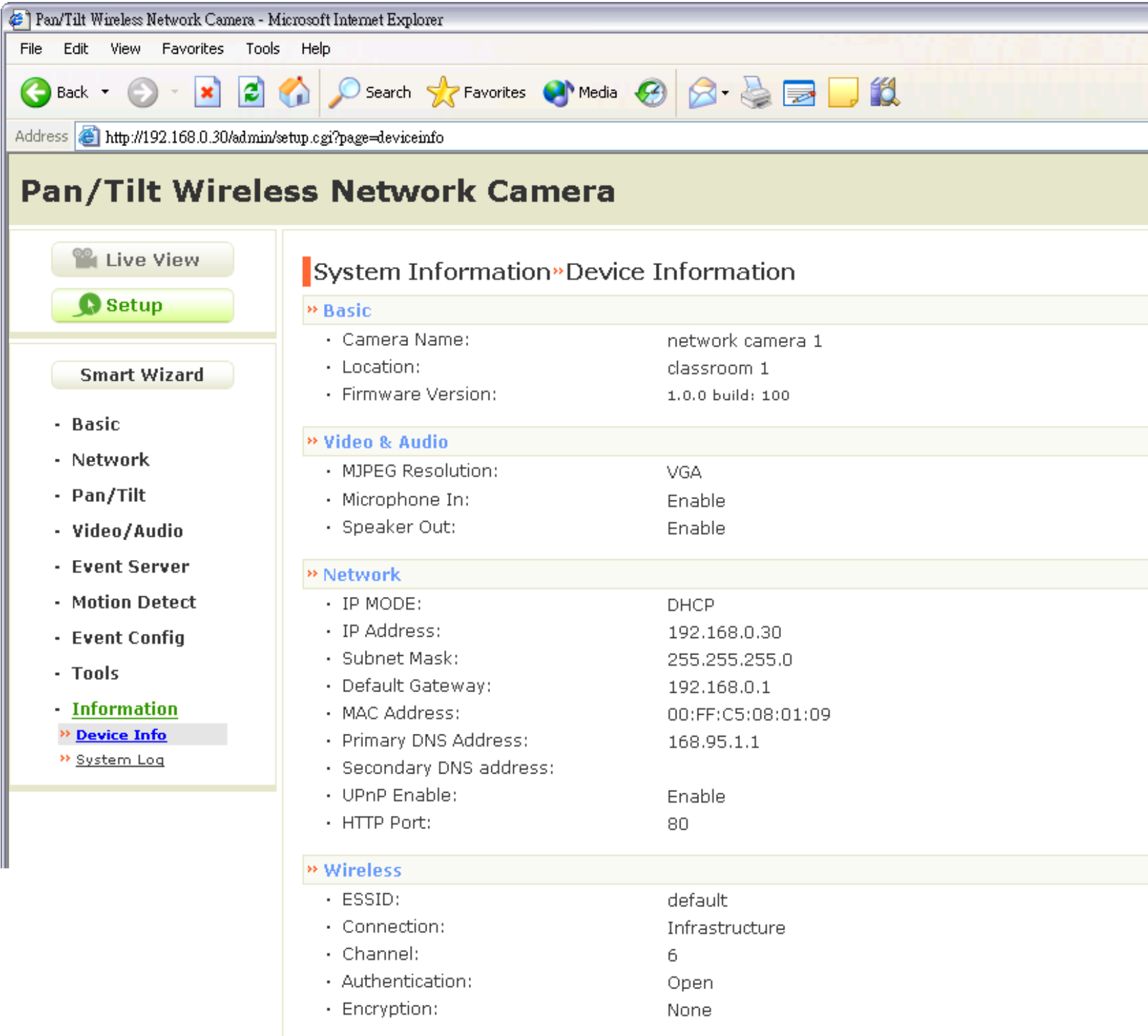
This item displays the current firmware version. You can upgrade the firmware for your camera once you obtained a latest version of firmware.

- **Select the firmware:** Click **Browse** to locate the backup file and then click **Update**.

NOTE Make sure to keep the camera connected to the power source during the process of upgrading firmware. Otherwise, the camera might be damaged because of failure of upgrading firmware.

4.11 Information

The Information menu displays the current configuration and events log of the camera.



■ Device Info

Display the Basic, Video & Audio, Network, and Wireless settings of the camera.

■ System Log

The Logs table displays the events log recorded by the system.

APPENDIX

A.1 Specification

■	Image Sensor	
	Sensor	1/4” color CMOS
	Resolution	640x480
■	Video	
	Compression	M-JPEG
	Video resolution	VGA/QVGA/QQVGA; 30fps max.
■	Audio	
	Input	Built-in MIC
	Output	Headphone output jack (Mono)
	Codec	PCM
■	User Interface	
	LAN	One RJ-45 port
	Antenna	One external antenna
	Reset	One Reset button
	GPIO	1 in/1 out connectors
		Input: active high: 9~40V DC; dropout: 0V DC
		Output: close circuit current 70mA AC or 100mA DC maximum, 30 Ohm; open circuit voltage 240V AC or 350V DC maximum
	LEDs	Power LED (amber); Link LED (green)
■	System Hardware	
	Processor	ARM9 base
	RAM	32MB SDRAM

ROM	4MB NOR Flash
Power	DC 12V
■ Communication	
LAN	10/100Mbps Fast Ethernet, auto-sensed, Auto-MDIX
WLAN	IEEE 802.11b/g
Protocol support	TCP/IP, UDP, ICMP, DHCP, NTP, DNS, DDNS, SMTP, FTP, PPPoE, UPnP
■ Pan/Tilt	
Pan	165 degree (left) to 165 degree (right)
Tilt	90 degree (up) to 15 degree (down)
■ Software	
OS Support	Windows 2000/XP/Vista
Browser	Internet Explorer 6.0 or above Apple Safari 2 or above Mozilla Firefox 2.00 or above
Software	UltraView for playback/recording/ configuration features
■ Operating Environment	
Temperature	- Operation: 0°C ~ 45°C - Storage: -15°C ~ 60°C
Humidity	- Operation: 20% ~ 85% non-condensing - Storage: 0% ~ 90% non-condensing
■ EMI	
	FCC Class B, CE Class B

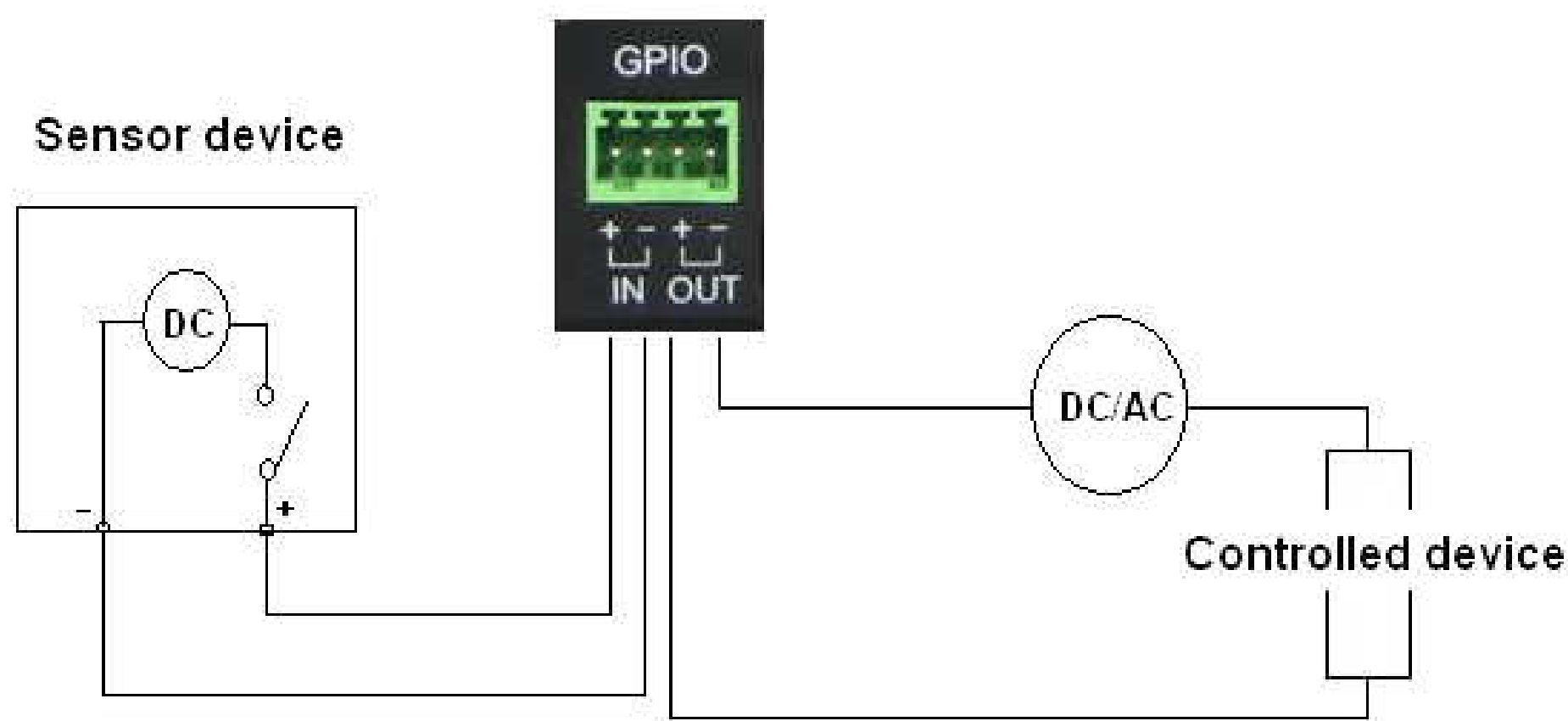
A.2 GPIO Terminal Application

This is typically used in association with programming scripts for developing applications for motion detection, event triggering, alarm notification via e-mail, and a variety of external control functions. The GPIO connectors are located on the rear panel of the camera, which provide the interface of connecting the sensor device (IN) and controlled device (OUT).

Connector Pin Assignment

PIN	SPECIFICATION
IN	Active High voltage 9~40V DC; Dropout-out voltage 0V DC
OUT	Close circuit current 70mA AC or 100mA DC maximum, Output resistance 30 Ohm; Open circuit voltage 240V AC or 350V DC maximum

Interface Schematic



A.3 Glossary of Terms

NUMBERS

10BASE-T	10BASE-T is Ethernet over UTP Category III, IV, or V unshielded twisted-pair media.
100BASE-TX	The two-pair twisted-media implementation of 100BASE-T is called 100BASE-TX.

A

ADPCM	Adaptive Differential Pulse Code Modulation, a new technology improved from PCM, which encodes analog sounds to digital form.
Applet	Applets are small Java programs that can be embedded in an HTML page. The rule at the moment is that an applet can only make an Internet connection to the computer from that the applet was sent.
ASCII	American Standard Code For Information Interchange, it is the standard method for encoding characters as 8-bit sequences of binary numbers, allowing a maximum of 256 characters.
ARP	Address Resolution Protocol. ARP is a protocol that resides at the TCP/IP Internet layer that delivers data on the same network by translating an IP address to a physical address.
AVI	Audio Video Interleave, it is a Windows platform audio and video file type, a common format for small movies and videos.

B

BOOTP	Bootstrap Protocol is an Internet protocol that can automatically configure a network device in a diskless workstation to give its own IP address.
--------------	--

C

Communication	Communication has four components: sender, receiver,
----------------------	--

message, and medium. In networks, devices and application tasks and processes communicate messages to each other over media. They represent the sender and receivers. The data they send is the message. The cabling or transmission method they use is the medium.

Connection

In networking, two devices establish a connection to communicate with each other.

D

DHCP

Developed by Microsoft, DHCP (Dynamic Host Configuration Protocol) is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. It also supports a mix of static and dynamic IP addresses. This simplifies the task for network administrators because the software keeps track of IP addresses rather than requiring an administrator to manage the task. A new computer can be added to a network without the hassle of manually assigning it a unique IP address. DHCP allows the specification for the service provided by a router, gateway, or other network device that automatically assigns an IP address to any device that requests one.

DNS

Domain Name System is an Internet service that translates domain names into IP addresses. Since domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses every time you use a domain name the DNS will translate the name into the corresponding IP address. For example, the domain name *www.network_camera.com* might translate to *192.167.222.8*.

E

Enterprise

An enterprise network consists of collections of networks connected to each other over a geographically dispersed

network	area. The enterprise network serves the needs of a widely distributed company and operates the company's mission-critical applications.
Ethernet	The most popular LAN communication technology. There are a variety of types of Ethernet, including 10Mbps (traditional Ethernet), 100Mbps (Fast Ethernet), and 1,000Mbps (Gigabit Ethernet). Most Ethernet networks use Category 5 cabling to carry information, in the form of electrical signals, between devices. Ethernet is an implementation of CSMA/CD that operates in a bus or star topology.
<u>E</u>	
Fast Ethernet	Fast Ethernet, also called 100BASE-T, operates at 10 or 100Mbps per second over UTP, STP, or fiber-optic media.
Firewall	Firewall is considered the first line of defense in protecting private information. For better security, data can be encrypted. A system designed to prevent unauthorized access to or from a private network. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially Intranets all messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.
<u>G</u>	
Gateway	A gateway links computers that use different data formats together.
Group	Groups consist of several user machines that have similar characteristics such as being in the same department.
<u>H</u>	
HEX	Short for hexadecimal refers to the base-16 number system,

which consists of 16 unique symbols: the numbers 0 to 9 and the letters A to F. For example, the decimal number 15 is represented as F in the hexadecimal numbering system. The hexadecimal system is useful because it can represent every byte (8 bits) as two consecutive hexadecimal digits. It is easier for humans to read hexadecimal numbers than binary numbers.

I

Intranet

This is a private network, inside an organization or company that uses the same software you will find on the public Internet. The only difference is that an Intranet is used for internal usage only.

Internet

The Internet is a globally linked system of computers that are logically connected based on the Internet Protocol (IP). The Internet provides different ways to access private and public information worldwide.

Internet address

To participate in Internet communications and on Internet Protocol-based networks, a node must have an Internet address that identifies it to the other nodes. All Internet addresses are IP addresses.

IP

Internet Protocol is the standard that describes the layout of the basic unit of information on the Internet (the *packet*) and also details the numerical addressing format used to route the information. Your Internet service provider controls the IP address of any device it connects to the Internet. The IP addresses in your network must conform to IP addressing rules. In smaller LANs, most people will allow the DHCP function of a router or gateway to assign the IP addresses on internal networks.

IP address

IP address is a 32-binary digit number that identifies each sender or receiver of information that is sent in packets across the Internet. For example, 80.80.80.69 is an IP address. When you “call” that number, using any connection methods, you get connected to the computer that “owns” that IP address.

ISP

ISP (Internet Service Provider) is a company that maintains a network that is linked to the Internet by way of a dedicated communication line. An ISP offers the use

of its dedicated communication lines to companies or individuals who can't afford the high monthly cost for a direct connection.

J

JAVA

Java is a programming language that is specially designed for writing programs that can be safely downloaded to your computer through the Internet without the fear of viruses. It is an object-oriented multi-thread programming best for creating applets and applications for the Internet, Intranet and other complex, distributed network.

L

LAN

Local Area Network. It is a computer network that spans a relatively small area sharing common resources. Most LANs are confined to a single building or group of buildings.

M

M-JPEG

M-JPEG (Motion JPEG) composes a moving image by storing each frame of a moving picture sequence in JPEG compression, and then decompressing and displaying each frame at rapid speed to show the moving picture.

N

NAT

Network Address Translator is generally applied by a router that makes many different IP addresses on an internal network appear to the Internet as a single address. For routing messages properly within your network, each device requires a unique IP address. But the addresses may not be valid outside your network. NAT solves the problem. When devices within your network request information from the Internet, the requests are forwarded to the Internet under the router's

IP address. NAT distributes the responses to the proper IP addresses within your network.

Network

A network consists of a collection of two or more devices, people, or components that communicate with each other over physical or virtual media. The most common types of network are:

LAN – (local area network): Computers are in close distance to one another. They are usually in the same office space, room, or building.

WAN – (wide area network): The computers are in different geographic locations and are connected by telephone lines or radio waves.

NWay Protocol

A network protocol that can automatically negotiate the highest possible transmission speed between two devices.

P

PCM

PCM (Pulse Code Modulation) is a technique for converting analog audio signals into digital form for transmission.

PING

Packet Internet Groper, a utility used to determine whether a specific IP address is accessible. It functions by sending a packet to the specified address and waits for a reply. It is primarily used to troubleshoot Internet connections.

PPPoE

Point-to-Point Protocol over Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as DSL or cable modem. All the users over the Ethernet share a common connection.

Protocol

Communication on the network is governed by sets of rules called protocols. Protocols provide the guidelines devices use to communicate with each other, and thus they have different functions. Some protocols are responsible for formatting and presenting data that will be transferred from file server memory to the file server's network adapter. Others are responsible for filtering

information between networks and forwarding data to its destination. Still other protocols dictate how data is transferred across the medium, and how servers respond to workstation requests and vice versa. Common network protocols responsible for the presentation and formatting of data for a network operating system are the Internetwork Packet Exchange (IPX) protocol or the Internet Protocol (IP). Protocols that dictate the format of data for transferors the medium include token-passing and Carrier Sense Multiple Access with Collision Detection (CSMA/CD), implemented as token-ring, ARCNET, FDDI, or Ethernet. The Router Information Protocol (RIP), a part of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite, forwards packets from one network to another using the same network protocol.

R

RJ-45

RJ-45 connector is used for Ethernet cable connections.

Router

A router is the network software or hardware entity in charge of routing packets between networks.

RTP

RTP (Real-time Transport Protocol) is a data transfer protocol defined to deliver **live media** to the clients at the same time, which defines the transmission of video and audio files in real time for Internet applications.

RTSP

RTSP (Real-time Streaming Protocol) is the standard used to transmit **stored media** to the client(s) at the same time, which provides client controls for random access to the content stream.

S

Server

It is a simple computer that provides resources, such as files or other information.

SIP

SIP (Session Initiated Protocol) is a standard protocol that delivers the real-time communication for Voice over IP (VoIP), which establishes sessions for features such as audio and video conferencing.

SMTP	The Simple Mail Transfer Protocol is used for Internet mail.
SNMP	Simple Network Management Protocol. SNMP was designed to provide a common foundation for managing network devices.
Station	In LANs, a station consists of a device that can communicate data on the network. In FDDI, a station includes both physical nodes and addressable logical devices. Workstations, single-attach stations, dual-attach stations, and concentrators are FDDI stations.
Subnet mask	In TCP/IP, the bits used to create the subnet are called the subnet mask.
<u>T</u> (TCP/IP)	Transmission Control Protocol/Internet Protocol is a widely used transport protocol that connects diverse computers of various transmission methods. It was developed by the Department of Defense to connect different computer types and led to the development of the Internet.
Transceiver	A transceiver joins two network segments together. Transceivers can also be used to join a segment that uses one medium to a segment that uses a different medium. On a 10BASE-5 network, the transceiver connects the network adapter or other network device to the medium. Transceivers also can be used on 10BASE-2 or 10BASE-T networks to attach devices with AUI ports.
<u>U</u> UDP	The User Datagram Protocol is a connectionless protocol that resides above IP in the TCP/IP suite
User Name	The USERNAME is the unique name assigned to each person who has access to the LAN.
Utility	It is a program that performs a specific task.
UTP	Unshielded twisted-pair. UTP is a form of cable used by

all access methods. It consists of several pairs of wires enclosed in an unshielded sheath.

W

WAN

Wide-Area Network. A wide-area network consists of groups of interconnected computers that are separated by a wide distance and communicate with each other via common carrier telecommunication techniques.

WEP

WEP is widely used as the basic security protocol in Wi-Fi networks, which secures data transmissions using 64-bit or 128-bit encryption.

Windows

Windows is a graphical user interface for workstations that use DOS.

WPA

WPA (Wi-Fi Protected Access) is used to improve the security of Wi-Fi networks, replacing the current WEP standard. It uses its own encryption, Temporal Key Integrity Protocol (TKIP), to secure data during transmission.

WPA2

Wi-Fi Protected Access 2. The latest security specification that provides greater data protection and network access control for Wi-Fi networks. WPA2 uses the government-grade AES encryption algorithm and IEEE 802.1X-based authentication, which are required to secure large corporate networks.